Convergence of Weighted Min-Sum Decoding
Via Dynamic Programming on Trees

Yung-Yih Jian and Henry D. Pfister
Department of Electrical and Computer Engineering, Texas A&M University
Email: {yungyih.jian,hpfister}@tamu.edu

Abstract

Applying the max-product (and belief-propagation) algorithms to loopy graphs is now quite popular for best assignment problems. This is largely due to their low computational complexity and impressive performance in practice. Still, there is no general understanding of the conditions required for convergence and/or the optimality of converged solutions. This paper presents an analysis of both attenuated max-product (AMP) decoding and weighted min-sum (WMS) decoding for LDPC codes which guarantees convergence to a fixed point when a weight parameter, $\beta$, is sufficiently small. It also shows that, if the fixed point satisfies some consistency conditions, then it must be both the linear-programming (LP) and maximum-likelihood (ML) solution.

For $(d_v, d_c)$-regular LDPC codes, the weight must satisfy $\beta(d_v - 1) \leq 1$ whereas the results proposed by Koetter and Frey require instead that $\beta(d_v - 1)(d_c - 1) < 1$. A counterexample which shows a fixed point might not be the ML solution if $\beta(d_v - 1) > 1$ is also given. Finally, connections are explored with recent work by Arora et al. on the threshold of LP decoding.

Index Terms

belief propagation, max product, min sum, LDPC codes, linear programming decoding

I. INTRODUCTION

The introduction of turbo codes in 1993 started a revolution in coding and inference that continued with the rediscovery of low-density parity-check (LDPC) codes and culminated in optimized LDPC codes

This work was supported in part by the National Science Foundation under Grant No. 0747470 and the Texas Norman Hackerman Advanced Research Program under Grant No. 00512-0168-2007. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.
that essentially achieve the capacity of practical channels [1], [2], [3], [4]. During this time, Wiberg et al. advanced the analysis of iterative decoding by proving a number of results for the min-sum (a.k.a. max-product) decoding algorithm [5], [6], [7]. Richardson and Urbanke also introduced the technique of density evolution (DE) to compute noise thresholds of message-passing decoding algorithms for turbo and LDPC codes [8].

For a particular noise realization, the optimality of iterative decoding solutions has also been considered by a number of authors. Weiss and Freeman have shown that the max-product (MP) assignment is locally optimal w.r.t. all single-loop and tree perturbations [9]. Unfortunately, this result is typically uninformative for LDPC codes with variables degrees larger than 2. Frey and Koetter have also shown that, with proper weights and adjustments, the attenuated max-product (AMP) decoding for LDPC codes returns the maximum-likelihood (ML) codeword if it converges to a codeword [7]. For general graphs, Wainwright et al. proposed the tree-reweighted max-product (TRMP) message-passing algorithm for computing the MAP assignment on the strictly positive Markov random field [10]. They have shown that, under some optimality conditions, the converged solution gives the MAP configuration for the graph. Their algorithm, though strictly different, has some similarity to the AMP algorithm in [7].

The linear programming (LP) decoding for LDPC codes, proposed by Feldman et al., solves a relaxed version of the ML decoding problem [11]. Since its introduction, a number of authors have looked for connections to the MP iterative decoding algorithm [12]. One interesting open question is, “What is the noise threshold of LP decoding?” The first threshold bound for LP decoding was proposed in [13]. Using expander graph arguments, they showed that LP decoding of a rate-$\frac{1}{2}$ regular LDPC code can correct all error patterns with weight less than 0.000175 of the block length. Since this is a worst-case analysis, the large gap to the empirical observations is not too surprising. Daskalakis et al. [14] were able to improve the threshold to 0.002 using probabilistic arguments based on a construction of a LP dual feasible solution. In [15], Koetter and Vontobel applied girth-based arguments to the dual LP problem. For a (3,6)-regular LDPC code, they proved that LP decoding can tolerate a crossover probability of $p = 0.01$ on the binary symmetric channel (BSC) and a noise level of $\sigma = 0.5574$ on the binary-input additive white Gaussian noise channel (BIAWGNC).

Arora et al. showed recently that, for a (3,6)-regular LDPC code, LP decoding can tolerate a crossover probability $p = 0.05$ on the BSC [16]. Instead of using a dual LP solution, they investigated the primal solution of the LP problem and proposed a local optimality condition for codewords. They proved that the local optimality implies both global optimality and LP optimality. So the probability that LP decoding succeeds is lower bounded by the probability that the correct codeword satisfies a set of local optimality
conditions. Since their local optimality conditions are amenable to analysis on tree-like neighborhoods, they perform a DE analysis to obtain BSC noise thresholds for LP decoding. Using DE for memoryless binary-input output symmetric (MBIOS) channels, Halabi et al. showed that LP decoding can achieve a noise threshold $\sigma = 0.735$ on the BIAWGNC [17].

The results in this paper can be seen as an extension of the work by Frey and Koetter that provides new insight into results of [15], [16]. We view both AMP and WMS [18] algorithms as computing the dynamic-programming (DP) solution to the optimal discounted-reward problem on a set of overlapping trees. This allows us to show that, for any received vector, the one-step update of the algorithm is a contraction on the space of message values when weight parameter is sufficiently small. From this, we deduce that the messages converge to a unique fixed point. We first show that, for $(d_v, d_c)$-regular LDPC codes, if the resulting fixed point satisfies some consistency conditions, then it must also be the LP optimum solution and, hence, the ML solution. Then, the WMS algorithm on $(d_v, d_c)$-regular LDPC codes with messages diverging to $\pm\infty$ is considered. We show that, for the weight $\beta = \frac{1}{d_v-1}$, if the WMS messages diverge to $\pm\infty$ and satisfies the consistency conditions, the corresponding hard decisions also return the ML solution.

The rest of the paper is organized as follows. Section III provides the background on factor graphs as well as the update rules of the AMP algorithm and the WMS algorithm. In Section III, we first investigate the convergence property of both algorithms, and introduce the consistency conditions for both algorithms. Then, the optimality of the hard decisions corresponding to the consistent fixed point is discussed. In Section IV the optimality of the codeword returned by the WMS algorithm when the messages are not converged is analyzed. A conjecture about the connections between noise thresholds of the WMS decoding and noise thresholds of the LP decoding is proposed in the same section. Numerical results are described and discussed in Section V. Finally, conclusions and extensions are given in Section VI.

II. BACKGROUND

A. Factor Graphs

An LDPC code can be defined by a bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{E}$ is the set of edges, and $\mathcal{V} = \mathcal{V}_L \cup \mathcal{V}_R$ consists of variable nodes (or bit nodes) $\mathcal{V}_L$ and check nodes (or constraint nodes) $\mathcal{V}_R$. In this paper, $(d_v, d_c)$-regular LDPC codes are considered. That is, each variable node in $\mathcal{V}_L$ has $d_v$ edges attached to it, and each check node in $\mathcal{V}_R$ has $d_c$ edges attached to it. For a set $\mathcal{S}$, let $|\mathcal{S}|$ denote the cardinality of $\mathcal{S}$. The number of variable nodes denoted by $n$ is $|\mathcal{V}_L|$. Any binary vector $x \in \{0, 1\}^n$ is
Therefore, finding the best assignment of the tree responding best assignment. Then, the solution of (1) is obtained by choosing root node of into two subproblems. For \( \beta \) where \( \mu \)

a codeword, or a valid assignment, if and only if it satisfies all check nodes in \( V_R \). We use \( C \) to denote the collection of all codewords. Let \( T^L_i \) be a computation tree of \( G \) which has depth \( L \) and is rooted at node \( i \). The set of vertices in the \( \ell \)th level of \( T^L_i \), where \( \ell \leq L \), is denoted by \( N(i, \ell) \). We also consider computation trees of \( G \) rooted at a directed edge \( i \rightarrow j \) or \( i \leftarrow j \) with \( (i, j) \in E \). For a graph \( G \), the size of the smallest cycle in \( G \) is denoted by \( \text{girth}(G) \). For a node \( i \in V \), we use \( N(i) \) to denote the set of neighbors of \( i \).

### B. Discounted Dynamic Programming on a Tree

Suppose that the computation tree \( T^L_i \) has depth \( 2L < \frac{1}{2} \text{girth}(G) \). Then, each node in \( T^L_i \) is associated with a different node in \( G \). Let \( I \subset V_L \) be the subset of variable nodes in \( T^L_i \). A binary vector \( w \in \{0, 1\}^n \) is a valid assignment on \( T^L_i \) if \( w \) satisfies all check nodes in \( T^L_i \). Let \( C_{T^L_i} \) be the set of all valid assignments on \( T^L_i \), and let \( C_{T^L_i}(x) \triangleq \{ w \in C_{T^L_i} : w_i = x, w_m = 0, \forall m \notin T^L_i \} \) be a subset of \( C_{T^L_i} \), where the assignment of the node \( m \in V_L \setminus I \) is 0 and the assignment of the root node is \( x \). In the remainder of this paper, we often simplify \( C_{T^L_i} \) to \( C_T \) when \( i \) and \( L \) are evident from the context. Similarly, we also simplify \( C_{T^L_i}(x) \) to \( C_T(x) \).

Let \( \gamma_i(x_i) \triangleq \log(p_{Y|X}(y_i|x_i)) \) be the log-likelihood of receiving \( y_i \in \mathbb{R} \) given that \( x_i \in \{0, 1\} \) is transmitted at the \( i \)th bit. We consider the problem of finding the best assignment \( w^* \in \{C_T(0) \cup C_T(1)\} \) to a tree \( T^L_i \) defined by

\[
\begin{align*}
  w^* & \triangleq \arg \max_{w \in \{C_T(0) \cup C_T(1)\}} \sum_{m \in I} \beta_m \gamma_m(w_m), \quad (1)
\end{align*}
\]

where \( \beta_m = \beta^L \) if \( m \in N(i, 2L) \) and 0 otherwise. Since \( C_T(0) \) and \( C_T(1) \) are disjoint, (1) can be separated into two subproblems. For \( x \in \{0, 1\} \), we first define a vector

\[
\begin{align*}
  w^*(x) & \triangleq \arg \max_{w \in C_T(x)} \sum_{m \in I} \beta_m \gamma_m(w_m), \quad (2)
\end{align*}
\]

and a function

\[
\begin{align*}
  \mu_i(x) & \triangleq \max_{w \in C_T(x)} \sum_{m \in I} \beta_m \gamma_m(w_m), \quad (3)
\end{align*}
\]

where \( \mu_i(x) \) is the optimal reward for assigning \( x \) to the root node of \( T^L_i \), and \( w^*(x) \) is the corresponding best assignment. Then, the solution of (1) is obtained by choosing \( w^*(x^*) \) where \( x^* = \arg \max_{x \in \{0, 1\}} \mu_i(x) \). Note that \( \mu_i(\cdot) \) is only a function of the assignment to the root node of \( T^L_i \). Therefore, finding the best assignment of the tree \( T^L_i \) is equivalent to finding the best assignment of the root node of \( T^L_i \).
The RHS in (3) can be rewritten as
\[ \mu_i(x) = \gamma_i(x) + \max_{w \in C_T(x)} \sum_{\ell=1}^{L} \sum_{m \in N(i,2\ell)} \beta^\ell \gamma_m(w_m). \] (4)

This suggests that we can compute \( \mu_i(x) \) recursively by using DP. In the \((\ell+1)\)th iteration, we compute the optimal discounted total reward \( \mu_{i \to j}^{(\ell+1)}(x) \) of assigning \( x \) to the directed edge \( i \to j \) by
\[ \mu_{i \to j}^{(\ell+1)}(x) = \gamma_i(x) + \beta \sum_{k \in N(i) \setminus j} \mu_{i \to k}^{(\ell)}(x) \]
\[ = \gamma_i(x) + \beta \sum_{k \in N(i) \setminus j} \max_{w \in S_{k,i}(x)} \sum_{m \in N(k) \setminus i} \mu_{m \to k}^{(\ell)}(w_m), \] (5)

where
\[ S_{k,i}(x) \triangleq \left\{ w \in \{0,1\}^n : w_i = x, \sum_{m \in N(k) \setminus i} w_m = 0 \mod 2 \right\} \] (6)
is the set of all valid assignments for variables in constraint \( k \) when \( x \) is assigned to the directed edge \( i \leftarrow k \). This follows from defining \( \mu_{i \to k}^{(\ell)}(x) \) to be the optimal discounted total reward for assigning \( x \) to the directed edge \( i \leftarrow k \) according to the rule
\[ \mu_{i \to k}^{(\ell)}(x) = \max_{w \in S_{k,i}(x)} \sum_{m \in N(k) \setminus i} \mu_{m \to k}^{(\ell)}(w_m). \] (7)

Finally, the reward function (4) can be computed by
\[ \mu_i(x) = \gamma_i(x) + \beta \sum_{j \in N(i)} \mu_{i \to j}^{(L)}(x). \]

To initialize the process, we choose \( \mu_{i \to j}^{(0)}(x) = \gamma_i(x) \) for all edges \( i \to j \) and all \( x \in \{0,1\} \). The update rule in (5) is the same as the AMP algorithm proposed in [7], where the optimal discounted total rewards \( \mu_{i \to j}^{(\ell)}(x) \) and \( \mu_{i \leftarrow j}^{(\ell)}(x) \) are the messages passed on the directed edges \( i \to j \) and \( i \leftarrow j \), respectively.

By using the update rule (5), one can compute \( \mu_i(x) \) for all \( i \in \mathcal{V}_L \) in parallel. Suppose that the total number of iterations \( L \) is less than \( \frac{1}{4}\text{girth}(\mathcal{G}) \). The vector \( \mathbf{x}^* \) with \( x^*_i = \arg \max_{x \in \{0,1\}} \mu_i(x) \) is the best assignments of the root of the trees \( \{T^{2L}_i : i \in \mathcal{V}_L \} \). Since \( T^{2L}_i \) for all \( i \in \mathcal{V}_L \) are overlapped, any variable node \( i \in \mathcal{V}_L \) appears in more than one tree. In both [7] and [16], it has been shown that if the best assignment of each \( i \in \mathcal{V}_L \) is consistent across all trees, then \( \mathbf{x}^* \) is the ML solution. To check the optimality of \( \mathbf{x}^* \), one has to first find the best assignment \( \mathbf{w}^* \) of each computation tree, and then test whether the assignment \( \mathbf{w}^* \) of each tree is consistent with \( \mathbf{x}^* \) or not. In this paper, we discuss how the weight factor \( \beta \) affects the decoder. We also propose other consistency conditions, which are easier to check, for regular LDPC codes. Finally, the analysis is extended to \( L > \frac{1}{4}\text{girth}(\mathcal{G}) \).
C. Attenuated Max-product Decoding Algorithm

In Section II-B, the original AMP algorithm was introduced. In this section, we introduce a modified version of the AMP algorithm, which is mathematically equivalent to the original one for any finite number of iterations.

Let $\gamma_i \triangleq \gamma_i(0) - \gamma_i(1)$ be the channel log-likelihood ratio (LLR) for the $i$th bit. It can be shown that $w^\ast(x)$ defined in (2) also maximizes the following objective function

$$\mu_i(x) = \sum_{w \in C_r(x), m \in I} \beta_m (1 - w_m) \gamma_m.$$  

(8)

To show the equivalence between the objective function of (2) and (8), we subtract a constant $\sum_{m \in I} \beta_m \gamma_m(1)$ from the objective function of (2). Then,

$$\arg \max_{w \in C_r(x)} \sum_{m \in I} \beta_m \gamma_m(w_m) = \arg \max_{w \in C_r(x)} \sum_{m \in I} \beta_m (\gamma_m(w_m) - \gamma_m(1))$$

$$= \arg \max_{w \in C_r(x)} \sum_{m \in I} \beta_m (1 - w_m) \gamma_m.$$ 

Therefore, the modified AMP update rule becomes

$$\mu^{(\ell+1)}_{i \rightarrow j}(x) = (1 - x)\gamma_i + \beta \sum_{k \in N(i) \setminus j} \mu^{(\ell)}_{i \leftarrow k}(x)$$

$$= (1 - x)\gamma_i + \beta \sum_{k \in N(i) \setminus j} \max_{w \in S_{u,i}(x)} \sum_{m \in N(k) \setminus i} \mu^{(\ell)}_{m \rightarrow k}(w_m),$$  

(9)

where the message $\mu^{(\ell+1)}_{i \rightarrow j}(x)$ now represents the weighted correlation between the LLRs and the best valid assignment with $x$ assigned to the directed edge $i \rightarrow j$. The algorithm starts by setting $\mu^{(0)}_{i \rightarrow j}(x) = (1 - x)\gamma_i$ for all $(i, j) \in E$ and all $x \in \{0, 1\}$.

Similar to the analysis in Section II-B, $\mu_{i \rightarrow j}(x)$ can be considered as a DP value function, that assigns a real number to each bit-to-check directed edge $i \rightarrow j$ and each possible assignment $x \in \{0, 1\}$. Based on the standard approach to DP, the update process can be seen as applying an operator $A : \mathbb{R}^{2|E|} \rightarrow \mathbb{R}^{2|E|}$ to messages. Let $\mu \in \mathbb{R}^{2|E|}$ with $\mu \triangleq \{\mu_{i \rightarrow j}(x) : (i, j) \in E, x \in \{0, 1\}\}$ be an AMP message vector. From (9), the operator $A$ is defined by $\nu = A[\mu]$ with

$$\nu_{i \rightarrow j}(x) = (1 - x)\gamma_i + \beta \sum_{k \in N(i) \setminus j} \mu_{i \leftarrow k}(x).$$

$$= (1 - x)\gamma_i + \beta \sum_{k \in N(i) \setminus j} \max_{w \in S_{u,i}(x)} \sum_{m \in N(k) \setminus i} \mu_{m \rightarrow k}(w_m).$$  

(10)

The AMP algorithm proceeds iteratively by computing $\mu^{(\ell+1)} = A[\mu^{(\ell)}]$. 


D. Weighted Min-sum Decoding Algorithm

Instead of passing the vector \( (\mu^{(\ell)}_{i \rightarrow j}(0), \mu^{(\ell)}_{i \rightarrow j}(1)) \in \mathbb{R}^2 \) as the \( i \rightarrow j \) message in the AMP algorithm, the WMS algorithm passes message \( \mu^{(\ell)}_{i \rightarrow j}(0) \triangleq \mu^{(\ell)}_{i \rightarrow j}(0) - \mu^{(\ell)}_{i \rightarrow j}(1) \), which is simply the difference between the best 0-root correlation and the best 1-root correlation. Similarly, the \( i \leftarrow j \) message is simplified to \( \mu^{(\ell)}_{i \leftarrow j} = \mu^{(\ell)}_{i \leftarrow j}(0) - \mu^{(\ell)}_{i \leftarrow j}(1) \). The update rules of the WMS algorithm are therefore given by

\[
\mu^{(\ell+1)}_{i \rightarrow j} = \gamma_i + \beta \sum_{k \in N(i) \setminus j} \mu^{(\ell)}_{i \leftarrow k},
\]

\[
\mu^{(\ell)}_{i \leftarrow j} = \left( \prod_{m \in N(j) \setminus i} \text{sgn} \left( \mu^{(\ell)}_{m \rightarrow j} \right) \right) \min_{m' \in N(j) \setminus i} |\mu^{(\ell)}_{m' \rightarrow j}|.
\]

It is easy to verify that the WMS algorithm is equivalent to the AMP algorithm.

Similar to the AMP algorithm, for any WMS message vector \( \mu \in \mathbb{R}^{|\mathcal{E}|} \) with \( \mu \triangleq \{ \mu_{i \rightarrow j} : (i, j) \in \mathcal{E} \} \), the update rule of the WMS algorithm can be seen as an operator \( W : \mathbb{R}^{|\mathcal{E}|} \rightarrow \mathbb{R}^{|\mathcal{E}|} \), which is defined by \( \nu = W[\mu] \) with

\[
\nu_{i \rightarrow j} = \gamma_i + \beta \sum_{k \in N(i) \setminus j} \left( \prod_{m \in N(j) \setminus i} \text{sgn} \left( \mu_{m \rightarrow j} \right) \right) \min_{m' \in N(j) \setminus i} |\mu_{m' \rightarrow j}|.
\]

The WMS algorithm is initialized by setting \( \mu^{(0)}_{i \rightarrow j} = \gamma_i \) and proceeds iteratively by computing \( \mu^{(\ell+1)} = W[\mu^{(\ell)}] \).

E. LP Decoding

Given the received vector \( y \in \mathbb{R}^n \), the ML decoder finds a codeword \( x^* \in \mathcal{C} \) such that the probability \( p(y|x^*) \) is maximal among all \( x \in \mathcal{C} \). Let \( \gamma \in \mathbb{R}^n \) be the vector of channel LLRs. Then, ML decoding can be defined as the following integer programming problem [11],

\[
\begin{align*}
\min & \quad \sum_{i=1}^n \gamma_i x_i \\
\text{subject to} & \quad x \in \mathcal{C}.
\end{align*}
\]

For a fixed graph \( G \), solving (14) directly is computationally infeasible for large \( n \) because the number of codewords grows exponentially in \( n \). In [11], a suboptimal decoder, i.e., LP decoder, was proposed. With the same objective function as in (14), the LP decoder searches the optimal solution over a relaxed polytope which is obtained by intersecting all local codeword polytopes defined by each check node of the graph \( G \).

Here, we briefly describe the LP decoder in [11] as follows. Given a check node \( j \in \mathcal{V}_R \), let

\[ \mathcal{E}_j = \{ S \subseteq N(j) : |S| \text{ is even} \} \]
be the collection of all support sets of local codewords for \( j \). Note that \( \emptyset \in E_j \) and represents the all-zeros codeword. For each \( j \in V_R \), and \( S \in E_j \), \( \zeta_{j,S} \) is an indicator function of the local codeword being assigned to \( j \). The LP decoder solves the following problem

\[
\begin{align*}
\min & \quad \sum_{i \in V_L} \gamma_i x_i \\
\text{subject to} & \quad \sum_{S \in E_j} \zeta_{j,S} = 1 \quad \forall j \in V_R \\
& \quad \sum_{S \in E_j \ S \ni i} \zeta_{j,S} = x_i \quad \forall (i, j) \in E \\
& \quad \zeta_{j,S} \geq 0, \quad x_i \geq 0 \quad \forall i \in V_L, \forall j \in V_R, \forall S \in E_j.
\end{align*}
\]

If the solution vector \( x^* \) is in \( \{0, 1\}^n \), then the vector \( x^* \) is an ML codeword. In the sequel, this LP problem is called \( \text{Problem-P} \).

To establish the dual problem of \( \text{Problem-P} \), a Lagrange multiplier \( \tau_{i,j} \) is associated with each edge \((i, j) \in E \) of the graph \( G \). The resulting dual problem is given by

\[
\begin{align*}
\max & \quad \sum_{j \in V_R} \tau_j \\
\text{subject to} & \quad \sum_{i \in S} \tau_{i,j} \geq \tau_j \quad \forall j \in V_R, \forall S \in E_j \\
& \quad \sum_{j \in N(i)} \tau_{i,j} \leq \gamma_i \quad \forall i \in V_L,
\end{align*}
\]

which, as shown in [15], is equivalent to

\[
\begin{align*}
\max & \quad \sum_{j \in V_R} \min_{S \in E_j} \sum_{i \in S} \tau_{i,j} \\
\text{subject to} & \quad \sum_{j \in N(i)} \tau_{i,j} = \gamma_i \quad \forall i \in V_L.
\end{align*}
\]

In the remainder of this paper, this dual problem is called \( \text{Problem-D} \).

Consider a \((d_v, d_c)\)-regular LDPC code, and let

\[
\mathcal{L} \triangleq \left\{ w \in \{0, 1\}^{d_c} : \sum_{i=1}^{d_c} w_i = 0 \mod 2 \right\}
\]

be the set of locally valid codewords. For each check node \( j \in V_R \), we define a vector \( \tau_j = \{ \tau_{i,j} : i \in N(j) \} \). Then the objective function in \( \text{Problem-D} \) can be written as \( \sum_{j \in V_R} \min_{w \in \mathcal{L}} \langle w, \tau_j \rangle \).

**F. Impossibility of a General ML Certificate for WMS Decoding**

In this section, two examples are provided for showing that WMS algorithm with some \( \beta > \frac{1}{d_c - 1} \) is not guaranteed to return an ML codeword.
Example 1. In this example, the ML optimality of the codeword returned by the WMS decoder with $\beta = 0.8$ is checked. We consider a $(3,4)$-regular LDPC code over the BSC channel with cross-over probability $p = 0.1$. The parity check matrix for the $(3,4)$-regular LDPC code is

$$H = \begin{pmatrix} 0, 0, 0, 1, 1, 0, 0, 0, 0, 1 \\ 0, 0, 0, 0, 1, 1, 1, 0, 1, 0 \\ 0, 1, 0, 0, 0, 0, 1, 0, 0, 0 \\ 1, 1, 1, 0, 0, 0, 0, 0, 0, 0 \\ 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 \\ 0, 0, 1, 0, 1, 1, 1, 0, 0, 1 \\ 1, 0, 0, 0, 1, 0, 1, 1, 0, 0 \\ 0, 1, 0, 0, 0, 0, 1, 0, 1, 1 \\ 0, 0, 1, 0, 0, 0, 0, 1, 1, 0 \end{pmatrix}.$$  

Since the codeword length is short ($n = 12$), we are able to implement the ML decoder defined in (14). For the WMS decoder, 200 iterations are performed in decoding each block. After testing $10^5$ blocks, there are 90905 codewords returned by the WMS decoder. Among these codewords returned by the WMS algorithm, only 90850 codewords are the ML codeword. Therefore, codewords returned by the WMS algorithm with $\beta = 0.8$ cannot be guaranteed to be ML optimal.

For the general case, the following example gives some intuition.

Example 2. Consider a $(d_v,d_c)$-regular LDPC code with codeword length $n$, where $d_c$ is an odd number and $d_v > 3$. Assume the all-zeros codeword is transmitted. Let the channel output LLR be $\gamma = (-1, \ldots, -1)$. Consider the WMS algorithm with $\beta > \frac{2}{d_v - 1}$.

At the beginning, all messages from variable nodes to their neighboring check nodes are $\mu_{i \rightarrow j}^{(0)} = -1$ for $i = 1, \ldots, n$ and $j \in N(i)$. Consider the message passed from the $j$th check node to its neighbor variable nodes, $\mu_{i \rightarrow j}$, $i \in N(j)$. Since the incoming messages are all equal to $-1$, the update rule of the WMS algorithm at the check node gives

$$\mu_{i \rightarrow j}^{(0)} = \left( \prod_{k \in N(j) \backslash i} \text{sgn}(\mu_{k \rightarrow j}) \right) \min_{k' \in N(j) \backslash i} |\mu_{k' \rightarrow j}^{(0)}| = 1,$$

for all $(i, j) \in \mathcal{E}$. In the first iteration, the outgoing message from the $i$th variable node to the $j$th check node is therefore

$$\mu_{i \rightarrow j}^{(1)} = \gamma_i + \beta \sum_{k \in N(i) \backslash j} \mu_{i \rightarrow k}^{(0)} > -1 + (d_v - 1) \frac{2}{d_v - 1} = 1.$$
Moreover, one can show that $\mu^{(\ell)}_{i \rightarrow j} \rightarrow \infty$ as $\ell \rightarrow \infty$. Thus, the hard decision output is an all-zeros codeword. Unfortunately, given this $\gamma$, we know that the ML output must be a nonzero codeword with maximal Hamming weight. Therefore, WMS algorithm cannot provide an ML certificate for $\beta > \frac{2}{d_v - 1}$. One might worry that this effect may be related to ties between ML codewords, but these can be avoided, without affecting the above result, by adding a very small amount of uniform random noise to the channel output LLRs.

### III. Convergence and Optimality Guarantees

In this section, the optimality of codewords obtained by the AMP algorithms and the WMS algorithms for LDPC codes is considered. We will show that the AMP algorithm converges to a fixed point when the weight factor $\beta(d_v - 1)(d_c - 1) < 1$. Further, if there is a codeword which satisfies the consistency conditions and uniquely maximizes the converged value functions, it can be shown that the codeword is the ML codeword. Similar to the analysis of the AMP decoding algorithm, we first discuss the convergence of the WMS algorithm. Compared to the convergence analysis of the AMP algorithm, a weaker condition for the convergence of the WMS algorithm, $\beta(d_v - 1) < 1$, is obtained. We also show that, if the converged messages satisfy the consistency conditions, which are similar to the conditions for the AMP algorithm, the optimality of the WMS codeword is guaranteed.

#### A. Attenuated Max-product Decoding Algorithm

Before showing that the AMP algorithm converges to a fixed point when $\beta < \frac{1}{(d_v - 1)(d_c - 1)}$, we first introduce the following tool lemma.

**Lemma 3.** For any two vectors $f, g \in \mathbb{R}^n$, the following inequality holds

$$\max_i |f_i - g_i| \geq \max_f \max_i |f_i - f_i'g_i'|. \tag{16}$$

**Proof:** See Appendix A.

**Theorem 4.** The operator $A$ is an $\|\cdot\|_\infty$ contraction on $\mathbb{R}^{2|E|}$ if

$$\beta < \frac{1}{(d_v - 1)(d_c - 1)}.$$  

**Proof:** Let $\mu, \nu \in \mathbb{R}^{2|E|}$ be two vectors of AMP messages, and let $\mu' = A[\mu]$ and $\nu' = A[\nu]$. By the definition of $A$ in (10) and the fact that for any two vectors $f$ and $g$ over $\mathbb{R}$, $|\sum_i (f_i - g_i)| \leq \sum_i |f_i - g_i|$, we have
\[ \|\mu' - \nu'\|_\infty \text{can be upper bounded by} \]
\[
\|\mu' - \nu'\|_\infty = \beta \max_{x \in \{0,1\}, (i,j) \in \mathcal{E}} \left| \sum_{k \in N(i) \setminus j} \mu_{i \leftarrow k}(x) - \sum_{k' \in N(i) \setminus j} \nu_{i \leftarrow k'}(x) \right|
\leq \beta \max_{x \in \{0,1\}, (i,j) \in \mathcal{E}} \sum_{k \in N(i) \setminus j} |\mu_{i \leftarrow k}(x) - \nu_{i \leftarrow k}(x)|.
\]  
(17)

From (7), the last term of the RHS in (17) can be rewritten as
\[
|\mu_{i \leftarrow k}(x) - \nu_{i \leftarrow k}(x)| = \left| \max_{w \in \mathcal{S}_k(x)} \sum_{m \in N(k) \setminus i} \mu_{m \rightarrow k}(w_m) - \max_{w' \in \mathcal{S}_k(x)} \sum_{m' \in N(k) \setminus i} \nu_{m' \rightarrow k}(w'_{m'}) \right|
\leq \max_{w \in \mathcal{S}_k(x)} \sum_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}(w_m) - \nu_{m \rightarrow k}(w_m)|
\leq \max_{w \in \mathcal{S}_k(x)} \sum_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}(w_m) - \nu_{m \rightarrow k}(w_m)|,
\]
where the inequality (a) follows by Lemma 3. Thus, the RHS in equation (17) is upper bounded by
\[
\beta \max_{x \in \{0,1\}, (i,j) \in \mathcal{E}} \sum_{k \in N(i) \setminus j} \max_{w \in \mathcal{S}_k(x)} \sum_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}(w_m) - \nu_{m \rightarrow k}(w_m)|.
\]  
(18)

Since \(\max(f + g) \leq \max g + \max f\), (18) is further upper bounded by
\[
\beta \sum_{k \in N(i) \setminus j} \max_{x \in \{0,1\}, (i,j) \in \mathcal{E}} \max_{w \in \mathcal{S}_k(x)} |\mu_{m \rightarrow k}(w_m) - \nu_{m \rightarrow k}(w_m)|
= \beta (d_v - 1)(d_c - 1) \max_{x \in \{0,1\}, (i,j) \in \mathcal{E}} |\mu_{i \rightarrow j}(x) - \nu_{i \rightarrow j}(x)|
\leq \|\mu - \nu\|_\infty,
\]
where the inequality (a) follows from the fact that \(\beta(d_c - 1)(d_v - 1) < 1\). This proves the theorem. \(\blacksquare\)

Remark 5. Combining Theorem 4 with the contraction mapping theorem shows that, for an arbitrary \((d_v, d_c)\)-regular LDPC code and any \(0 < \beta < \frac{1}{(d_v - 1)(d_c - 1)}\), the AMP algorithm converges to a unique fixed point denoted by \(\mu^*\). That is \(\mu^{(\ell)} \rightarrow \mu^*\) as \(\ell \rightarrow \infty\), and \(\mu^* = A[\mu^*]\). We note that this idea is very similar to the existence proof for optimal stationary policies of discounted Markov decision processes.

For each \((i,j) \in \mathcal{E}\), let \(x^*_{i,j} \in \{0,1\}\) be the assignment which uniquely maximizes \(\mu^*_{i \rightarrow j}(x)\), and let \(x^* \in \{0,1\}^n\) be the vector returned by the AMP algorithm. For regular LDPC codes, it suffices to show the ML optimality of \(x^*\) if the following conditions hold.

Definition 6 (AMP-consistency). The assignment \(\{x^*_i : (i,j) \in \mathcal{E}\}\) is called AMP-consistent if \(x^* \in C\), \(x^*_{i,j} = x^*_i\).
Lemma 7. Consider a \((d_v, d_c)\)-regular LDPC code, and choose \(\beta < \frac{1}{(d_c-1)(d_v-1)}\). For each edge \((i, j) \in \mathcal{E}\), let \(\mu_{i \rightarrow j}^*(x)\) be the fixed point, and let \(x_{i,j}^*\) uniquely maximize \(\mu_{i \rightarrow j}^*(x)\). Then for any binary vector \(\{x_{i,j}\} \in \{0, 1\}^{|\mathcal{E}|}\),
\[
\sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x_{i,j}) \leq \sum_{(i,j) \in \mathcal{E}} (1 - x_{i,j}) \gamma_i + \beta (d_v - 1) (d_c - 1) \sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x_{i,j}^*),
\]
with equality if and only if \(\{x_{i,j}^*: (i,j) \in \mathcal{E}\}\) is AMP-consistent, and \(x_{i,j} = x_{i,j}^*\) for all \((i,j) \in \mathcal{E}\).

Proof: See Appendix \[B\]

Remark 8. From Lemma \[7\], we know that when the assignment \(\{x_{i,j}^*\}\) is AMP-consistent, then
\[
\sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x_{i,j}^*) = \frac{d_v \sum_{i \in \mathcal{V}_k} (1 - x_i^*) \gamma_i}{1 - \beta (d_v - 1) (d_c - 1)},
\]
where \(x_i^* = x_{i,j}^*\) for all \(i \in \mathcal{V}_L\) and \((i,j) \in \mathcal{E}\).

Theorem 9. Given the LLR vector \(\gamma \in \mathbb{R}^n\), let the assignment \(x_{i,j}^*\) uniquely maximize \(\mu_{i \rightarrow j}^*(x)\) for all \((i,j) \in \mathcal{E}\). If \(\{x_{i,j}^*: (i,j) \in \mathcal{E}\}\) is AMP-consistent, then \(x^* = \{x_i^*: i \in \mathcal{V}_L\}\) is the ML codeword.

Proof: We prove that \(x^*\) is the ML codeword by showing that \(x^*\) uniquely maximizes the correlation \(\sum_{i \in \mathcal{V}_L} (1 - x_i^*) \gamma_i\) over all codewords in \(\mathcal{C}\).

Consider any codeword \(\tilde{x} \in \mathcal{C}\) such that \(\tilde{x} \neq x^*\), and \(\{\tilde{x}_{i,j}\} \in \{0, 1\}^{|\mathcal{E}|}\) be the corresponding binary vector with \(\tilde{x}_{i,j} = \tilde{x}_j\) for all \(j \in N(i)\). From (9), we know
\[
\sum_{(i,j) \in \mathcal{E}} (1 - \tilde{x}_{i,j}) \gamma_i = \sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (\tilde{x}_{i,j}) - \beta \sum_{(i,j) \in \mathcal{E}} \max_{\tilde{x}_{i,j} \in \mathcal{S}_{k,i}(\tilde{x}_{i,j})} \sum_{m \in N(k) \setminus i} \mu_{m \rightarrow k}^* (w_m).
\]
By the fact that \(\tilde{x}\) is also in \(\mathcal{S}_{k,i}(\tilde{x}_{i,j})\), we have
\[
\max_{\tilde{x}_{i,j} \in \mathcal{S}_{k,i}(\tilde{x}_{i,j})} \sum_{m \in N(k) \setminus i} \mu_{m \rightarrow k}^* (w_m) \geq \sum_{m \in N(k) \setminus i} \mu_{m \rightarrow k}^* (\tilde{x}_{m,k}).
\]
Therefore, the RHS in (20) is upper bounded by
\[
\sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (\tilde{x}_{i,j}) - \beta \sum_{(i,j) \in \mathcal{E}, k \in N(i) \setminus j} \mu_{m \rightarrow k}^* (\tilde{x}_{m,k})
\]
\[
= (1 - \beta (d_v - 1) (d_c - 1)) \sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (\tilde{x}_{i,j}).
\]
Since \(x_{i,j}^*\) uniquely maximizes \(\sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x)\), the RHS in (21) is less than
\[
(1 - \beta (d_v - 1) (d_c - 1)) \sum_{(i,j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x_{i,j}^*).
\]
Thus, we have
\[
\sum_{i \in \mathcal{V}_L} (1 - \tilde{x}_i) \gamma_i < \frac{1}{d_v} (1 - \beta (d_v - 1) (d_c - 1)) \sum_{(i, j) \in \mathcal{E}} \mu_{i \rightarrow j}^* (x_{i, j}^*)
\]
\[= (a) \sum_{i \in \mathcal{V}_L} (1 - x_i^*) \gamma_i,
\]
where (a) follows from (19). This shows that $x^*$ uniquely maximizes the correlation $\sum_{i \in \mathcal{V}_L} (1 - x_i) \gamma_i$ over all $x \in \mathcal{C}$ and is therefore the ML codeword.

**B. Weighted Min-sum Decoding Algorithm**

Before showing the optimality of the WMS algorithm, we first introduce a consistency condition for WMS decoding.

**Definition 10 (WMS-consistency).** Let $\mu_{i \rightarrow j}^{(\ell)}$ be the message passed from the $i$th bit to the $j$th check in the $\ell$th iteration, and $\mu_{i \leftarrow j}^{(\ell)}$ be the message passed from $j$th check to $i$th bit, defined in (12). The message vector $\mu^{(\ell)}$ is called **WMS-consistent** if, for each bit $i \in \mathcal{V}_L$, it satisfies 1) $\text{sgn}(\mu_{i \rightarrow j}^{(\ell)}) = \text{sgn}(\mu_{i \rightarrow j'}^{(\ell)})$ for $j, j' \in N(i)$, 2) $\text{sgn}(\mu_{i \leftarrow j}^{(\ell)}) = \text{sgn}(\mu_{i \leftarrow j}^{(\ell)})$ for $j \in N(i)$, and 3) $\text{sgn}(\gamma_i + \beta \sum_{j \in N(i)} \mu_{i \leftarrow j}^{(\ell)}) = \text{sgn}(\mu_{i \rightarrow j'}^{(\ell)})$ for $j' \in N(i)$.

When the WMS messages satisfy the WMS-consistency conditions, the following theorem shows that the corresponding hard decisions return a codeword.

**Theorem 11.** If the WMS messages in the $\ell$th iteration are WMS-consistent, then the hard decisions
\[
\hat{x}_i = \frac{1}{2} \left(1 - \text{sgn} \left( \gamma_i + \beta \sum_{j \in N(i)} \mu_{i \leftarrow j}^{(\ell)} \right) \right)
\]
for $i = 1, \ldots, n$ give a codeword.

**Proof:** We prove this result by contradiction. Assume that $\hat{x}$ is not a codeword. There exists at least one unsatisfied parity check node. Let $j \in \mathcal{V}_R$ be the unsatisfied parity check node and $N(j)$ be the neighbors of $j$. Since $\sum_{i \in N(j)} \hat{x}_i = 1 \mod 2$, we have
\[
-1 = \prod_{i \in N(j)} \text{sgn} \left( \gamma_i + \beta \sum_{j' \in N(i)} \mu_{i \leftarrow j'}^{(\ell)} \right) = \prod_{i \in N(j)} \text{sgn} \left( \mu_{i \rightarrow j}^{(\ell)} \right).
\]
Consider the message passed from the $j$th check to the $i$th bit. From the WMS update rule,

$$
\mu_i^{(\ell)} \leftarrow \prod_{m \in \mathcal{N}(j) \setminus i} \text{sgn} \left( \mu_{m \rightarrow j}^{(\ell)} \right) \times \min_{m \in \mathcal{N}(j) \setminus i} \left| \mu_{m \rightarrow j}^{(\ell)} \right| 
= - \text{sgn} \left( \mu_i^{(\ell)} \right) \times \min_{m \in \mathcal{N}(j) \setminus i} \left| \mu_{m \rightarrow j}^{(\ell)} \right|.
$$

This contradicts the condition 2) of WMS-consistency.

Next, we consider the optimality of the solution returned by the WMS decoder. Similar to the analysis of the AMP algorithm, we first discuss the convergence of the WMS messages. When the WMS messages converge to a fixed point, we show that the corresponding hard decisions give an optimal codeword if the fixed point is WMS-consistent.

To show the convergence of the WMS algorithm, we first introduce the following lemma.

**Lemma 12.** Consider two WMS message vectors $\mu, \nu \in \mathbb{R}^{|\mathcal{E}|}$. Let $i \in \mathcal{V}_L$, $k \in \mathcal{V}_R$ and $(i, k) \in \mathcal{E}$, and define

$$
d_{i,k} \triangleq \left| \left( \prod_{m \in \mathcal{N}(k) \setminus i} \text{sgn} \left( \mu_{m \rightarrow k} \right) \right) \min_{m' \in \mathcal{N}(k) \setminus i} \left| \mu_{m' \rightarrow k} \right| - \left( \prod_{m \in \mathcal{N}(k) \setminus i} \text{sgn} \left( \nu_{m \rightarrow k} \right) \right) \min_{m' \in \mathcal{N}(k) \setminus i} \left| \nu_{m' \rightarrow k} \right| \right|.
$$

Then,

$$
\max_{m \in \mathcal{N}(k) \setminus i} \left| \mu_{m \rightarrow k} - \nu_{m \rightarrow k} \right| \geq d_{i,k}.
$$

*Proof:* See Appendix C.

To show the convergence of the WMS messages, it will suffice to show that the WMS operator $W$ is an $\| \cdot \|_{\infty}$ contraction. The following theorem provides a precise statement.

**Theorem 13.** For all LLR vectors and message vectors, the WMS operator $W$ is an $\| \cdot \|_{\infty}$ contraction if

$$
\beta (d_v - 1) < 1.
$$

*Proof:* Using Lemma 12 one can upper bound $\| W[\mu] - W[\nu] \|_{\infty}$ in a straightforward manner to
get
\[ \|W[\mu] - W[\nu]\|_{\infty} \leq \max_{(i,j)\in\mathcal{E}} \beta \sum_{k\in\mathcal{N}(i)\setminus j} d_{i,k} \]
\[ \leq \beta (d_v - 1) \max_{(i,k)\in\mathcal{E}} d_{i,k} \]
\[ \leq \beta (d_v - 1) \max_{(i,k)\in\mathcal{E}} \left| \mu_{m\rightarrow k} - \nu_{m\rightarrow k} \right| \]
\[ = \beta (d_v - 1) \|\mu - \nu\|_{\infty}. \]

This implies that \( W \) is a \( \|\cdot\|_{\infty} \) contraction.

**Remark 14.** Combining this with the contraction mapping theorem shows that, for an arbitrary \((d_v, d_c)\)-regular LDPC code and any \(0 \leq \beta < \frac{1}{d_v-1}\), the WMS algorithm converges to a unique fixed point, \(\mu^{(t)}_{i\rightarrow j} \rightarrow \mu^*_{i\rightarrow j} \) and \(\mu^{(t)}_{i\leftarrow j} \rightarrow \mu^*_{i\leftarrow j}\), as the number of iterations goes to infinity.

For any WMS-consistent fixed point, there are two ways to prove the optimality of the hard decision output. One way is by looking at Problem-\(P\) directly, which has been shown in our earlier work [19]. We generalize the definition of minimal \(T\)-local deviation in [16] to \(T \geq \frac{1}{4}\text{girth}(G)\). By using the generalized minimal \(T\)-local deviation, it can be shown that, if the fixed point is WMS-consistent, the corresponding hard decision bits also return a locally optimal codeword. By the fact that local optimality implies global optimal and LP optimal, the hard decision is an LP and ML codeword. A summary of [19] is provided in Appendix [F].

The other method, which is introduced in the rest of this section, is by examining the optimality in Problem-\(D\). We construct a dual witness according to the method introduced in [15]. The following lemma shows that the vector \(\tau^* \in \mathbb{R}^{|\mathcal{E}|}\), which is constructed from the fixed-point messages \(\mu^*_{i\rightarrow j}\) and \(\mu^*_{i\leftarrow j}\), is a dual feasible point of Problem-\(P\).

**Lemma 15.** Consider the WMS algorithm with \(\beta < \frac{1}{d_v-1}\) over a \((d_v, d_c)\)-regular LDPC code. The vector \(\tau^* \in \mathbb{R}^{|\mathcal{E}|}\) defined by

\[ \tau_{i,j}^* = \frac{1}{d_v} \left( \mu_{i\rightarrow j}^* - \beta (d_v - 1) \mu_{i\leftarrow j}^* \right) \tag{22} \]

is a dual feasible point of Problem-\(P\).

**Proof:** Fix a variable node \(i \in \mathcal{V}_L\). The sum of the dual variables on the edges incident to \(i\) is given
This proves the lemma. \(\blacksquare\)

**Remark 16.** Compared to the construction in [15], Lemma 15 is a simplified version by just considering one-step update of the WMS messages. In [15], min-sum messages over \(L\) iterations are considered. For a computation tree \(T_j^{2L}\) of depth \(2L\) rooted at check node \(j\), those min-sum messages are used to generate an assignment \(\tau(j, L)\) to edges in \(T_j^{2L}\). Koetter and Vontobel showed that the dual feasible point \(\tau^*\) can be obtained by averaging \(\tau(j, L)\) over all \(j \in \mathcal{V}_R\). Since the number of leaf nodes in a computation tree increases doubly exponentially, a weight factor \(\alpha\) is introduced to attenuate the influence of the leaves of the computation tree. In our analysis, by the fact that the WMS messages satisfy a fixed-point equation, we simplify the construction and consider only the assignments on the top level of computation tree. Next, we will show that the proposed dual-feasible point \(\tau^*\) is also a dual-optimal point in Problem-D if it is constructed from a WMS-consistent fixed point.

For a \(j \in \mathcal{V}_R\), let \(\tau_j^* \in \mathbb{R}^{d_c}\) denote the assignments on the edges incident to \(j\), \(\{\tau_{i,j}^*: i \in N(j)\}\), and let \(\mu_j^* = \{\mu_{i,j}^*: i \in N(j)\}\) be the set of messages to \(j\). Without loss of generality, we can sort the vertices in \(N(j)\) by \((i_1, i_2, \ldots, i_{d_c})\) such that \(|\mu_{i_1,j}^*| \leq |\mu_{i_2,j}^*| \leq \cdots \leq |\mu_{i_{d_c},j}^*|\). With this order, \(\tau_j^*\) is rearranged into a vector \(t \in \mathbb{R}^{d_c}\), where \(t_k = \tau_{i_k,j}^*\). Also, we define two vectors \(\vec{\mu}, \mu \in \mathbb{R}^{d_c}\) with \(\vec{\mu}_k = \mu_{i_k,j}^*\) and \(\mu_k = \mu_{i_{d_k},j}^*\) for \(k = 1, 2, \ldots, d_c\), respectively. Given a vector \(f\), we use \(\text{sgn}(f)\) to denote a vector which is composed of the sign of each entry in \(f\). Finally, we use \(1\) to represent an all-one vector, and the dimension is determined in the context of equations.

The following lemma shows that an affine function of \(\text{sgn}(\mu_j^*)\) minimizes the inner product \(\langle w, t \rangle\) for all \(w \in \mathcal{L}\) when the fixed point is WMS-consistent. Recall that \(\mathcal{L}\) is defined in [15].

**Lemma 17.** Consider a \((d_v, d_c)\)-regular LDPC code. For some \(j \in \mathcal{V}_R\), if the WMS algorithm with \(\beta < \frac{1}{d_v - 1}\) converges to a WMS-consistent fixed point \(\mu_{i,j}^*\) and \(\mu_{i,j}^*\) for all \((i, j) \in \mathcal{E}\), then

\[
\arg \min_{w \in \mathcal{L}} \langle w, \tau_j^* \rangle = \frac{1}{2} (1 - \text{sgn}(\mu_j^*)). \tag{23}
\]
Proof: Since messages are WMS-consistent, we know that the RHS in (23) satisfies the \( j \)th check node from Theorem 11. From (22), the LHS in (23) can be rewritten as
\[
\langle w, \tau^*_j \rangle = \sum_{k=1}^{d_v} w_k t_k
\]
\[
= \frac{1}{d_v} \sum_{k=1}^{d_v} w_k \left( \vec{\mu}_k - \beta (d_v - 1) \vec{\mu}_k \right)
\]
\[
= \frac{1}{d_v} \sum_{k=1}^{d_v} w_k \text{sgn} \left( \vec{\mu}_k \right) \left( \left| \vec{\mu}_k \right| - \beta (d_v - 1) \left| \vec{\mu}_k \right| \right),
\]  
(24)
where the equality (a) holds by condition 2) of WMS-consistency. From the update rule of the WMS algorithm, one can show that
\[
\left| \vec{\mu}_k \right| = \begin{cases} 
\left| \vec{\mu}_2 \right|, & \text{when } k = 1, \\
\left| \vec{\mu}_1 \right|, & \text{otherwise}.
\end{cases}
\]
Thus, the summation in (24) becomes
\[
\frac{1}{d_v} w_1 \text{sgn} \left( \vec{\mu}_1 \right) \left( \left| \vec{\mu}_1 \right| - \beta (d_v - 1) \left| \vec{\mu}_2 \right| \right)
\]
\[
+ \frac{1}{d_v} \sum_{k=2}^{d_v} w_k \text{sgn} \left( \vec{\mu}_k \right) \left( \left| \vec{\mu}_k \right| - \beta (d_v - 1) \left| \vec{\mu}_1 \right| \right).
\]
Since \( 0 \leq \beta (d_v - 1) < 1 \), one can show that
\[
\left| \left| \vec{\mu}_1 \right| - \beta (d_v - 1) \left| \vec{\mu}_2 \right| \right| \leq \left| \left| \vec{\mu}_k \right| - \beta (d_v - 1) \left| \vec{\mu}_1 \right| \right|
\]
for \( k \geq 2 \). Thus, the minimum is achieved by choosing
\[
w_k = \begin{cases} 
\frac{1}{2} \left( 1 - \text{sgn} \left( \vec{\mu}_k \right) \right) & \text{for } k = 2, 3, \ldots, d_v, \\
\sum_{m=2}^{d_v} w_m \mod 2 & \text{for } k = 1.
\end{cases}
\]
By the fact that \( \frac{1}{2} (1 - \text{sgn}(\vec{\mu}_j)) \) satisfies the \( j \)th check node, thus \( w_1 = \frac{1}{2} (1 - \text{sgn}(\vec{\mu}_1)) = \frac{1}{2} (1 - \text{sgn}(\vec{\mu}_{1 \rightarrow j})) \). This completes the proof.

Remark 18. The proof of Lemma 17 employs part of the observation in the proof of [15, Lemma 3]. Given a check node, the absolute values of all but one outgoing WMS messages are the same. The only different absolute value of the outgoing message will be passed along the edge that the smallest absolute value of incoming message was passed on. With this observation, we know that the corresponding binary value \( w_1 \) will depend on the other binary values \( w_2, \ldots, w_{d_v} \). Since min-sum messages are not guaranteed to converge, Koetter and Vontobel computed the dual feasible point using computation trees of depth
greater than one. In order to offset the influence of the exponential weighting of the messages from the leaf nodes, a large initial value assumption is required. With this large initial value assumption, they showed that the constructed dual feasible point is an optimal point in Problem-D.

Let $\tau \in \mathbb{R}^{|E|}$ and $g(\tau)$ be the objective function in Problem-D. Let $w^{(j)} \triangleq \frac{1}{2}(1 - \text{sgn}(\mu^{*}_{j}))$ be the local assignment to check $j$. By Lemma 15 and Lemma 17, one can show that the optimal value of the objective function in Problem-D given $\tau^{*}$ is

$$g(\tau^{*}) = \sum_{j \in \mathcal{V}_{R}} \langle \tau^{*}_{j}, w^{(j)} \rangle.$$ 

To find the optimal solution of Problem-D, one needs to search over all $\tau$ in the dual-feasible set and find the maximum of $g(\tau)$. Let the optimal value of Problem-P and the optimal value of Problem-D be $f^{*}$ and $g^{*}$, respectively. Since $\tau^{*}$ is in the feasible set of Problem-D, it is obvious that $g^{*} \geq g(\tau^{*})$. In the following theorem, we show that if the fixed point $\mu^{*} \triangleq \{\mu^{*}_{i \rightarrow j} : (i, j) \in \mathcal{E}\}$ is WMS-consistent, the proposed dual-feasible point $\tau^{*}$ actually achieves the maximum, that is, $g^{*} = g(\tau^{*})$. Also, the corresponding hard decisions return an optimal codeword, i.e., an ML codeword.

**Theorem 19.** Consider the WMS algorithm with $\beta < \frac{1}{d_{v} - 1}$. If the message vector $\mu^{(t)}$ converges to a WMS-consistent fixed point, $\mu^{*}$, then the hard decision bits $x^{*} \in \{0, 1\}^{n}$ with

$$x^{*}_{i} = \frac{1}{2} \left(1 - \text{sgn} \left(\gamma_{i} + \beta \sum_{j \in \mathcal{N}(i)} \mu^{*}_{i \rightarrow j}\right)\right)$$

is a codeword. Also, $x^{*}$ is LP optimal and, hence, ML optimal.

**Proof:** Let $\tau^{*}$ be a dual feasible point constructed as proposed in Lemma 15. Let $w^{(j)} \in \mathcal{L}$ be the binary vector that minimizes the inner product $\langle w, \tau^{*}_{j} \rangle$ over all $w \in \mathcal{L}$. Then, from Lemma 17 we know $w^{(j)} = \frac{1}{2}(1 - \text{sgn}(\mu^{*}_{j}))$ for each $j \in \mathcal{V}_{R}$. Since the fixed point $\mu^{*}$ is WMS-consistent, by Theorem 11 it can be shown that $w^{(j)} = \{x^{*}_{i} : i \in \mathcal{N}(j)\}$, where $x^{*}_{i} = \frac{1}{2}(1 - \text{sgn}(\gamma_{i} + \beta \sum_{j \in \mathcal{N}(i)} \mu^{*}_{i \rightarrow j}))$ is the hard decision of the $i$th bit.

In the following proof, we will show that $x^{*}$ is LP optimal by contradiction. Assume that $x^{*}$ does not minimize Problem-P, then we have

$$f^{*} < \sum_{i \in \mathcal{V}_{L}} \gamma_{i} x^{*}_{i} = \sum_{i \in \mathcal{V}_{L}} \left(\sum_{j \in \mathcal{N}(i)} \tau^{*}_{i,j} \right) x^{*}_{i} = \sum_{j \in \mathcal{V}_{R}} \left(\sum_{i \in \mathcal{N}(j)} \tau^{*}_{i,j} x^{*}_{i} \right) = \sum_{j \in \mathcal{V}_{R}} \langle \tau^{*}_{j}, w^{(j)} \rangle = g(\tau^{*}) \leq g^{*},$$

which contradicts the assumption that $x^{*}$ is not LP optimal.
where (a) follows from Lemma [15] and (b) is a result of the WMS-consistency conditions. But, weak duality implies that \( f^* \geq g^* \), and this gives a contradiction. Thus, \( x^* \) minimizes the primal problem, and hence, is LP optimal. Moreover, since \( x^* \in C \), it is also an ML codeword.

\[ \text{Remark 20. Consider the WMS algorithm on a} \ (d_v, d_c) \text{-regular LDPC code with} \ \beta < \frac{1}{d_v - 1}. \text{From Theorem [19] we are able to check the optimality of the WMS solution by testing the WMS-consistency conditions. If the messages satisfy the consistency conditions, then the hard decision bits return an ML codeword.} \]

IV. Weighted Min-sum Decoding with \( \beta = \frac{1}{d_v - 1} \)

We first introduce some notation and definitions. We denote the WMS messages \( \{ \mu_{i\rightarrow j}^{(\ell)} : (i, j) \in \mathcal{E} \} \) with \( \beta = \frac{1}{d_v - 1} \) in the \( \ell \)th iteration by a vector \( \mu^{(\ell)} \in \mathbb{R}^{|\mathcal{E}|} \). The hard decisions computed by \( \mu^{(L_0)} \) are denoted by a binary vector \( x^{(L_0)} \in \{0, 1\}^n \). For the WMS algorithm with \( \beta = \frac{\delta}{d_v - 1} \) and \( 0 \leq \delta < 1 \), we use the vectors \( \mu_{i}^{(\ell)} \in \mathbb{R}^{|\mathcal{E}|} \) and \( \mu_{i}^{*} \in \mathbb{R}^{|\mathcal{E}|} \) to denote the messages in the \( \ell \)th iteration and the fixed-point messages, respectively. The collection of hard decision bits computed using \( \mu_{i}^{*} \) is denoted by a vector \( x_{i}^{*} \in \{0, 1\}^n \). Moreover, for any WMS message vector \( \mu \in \mathbb{R}^{|\mathcal{E}|} \), the vector \( |\mu| \in \mathbb{R}^{|\mathcal{E}|} \) consists of the absolute value of each element of \( \mu \). For any two WMS message vectors \( \mu, \nu \in \mathbb{R}^{|\mathcal{E}|} \), we use \( \mu \triangleright \nu \) to denote that \( \text{sgn}(\mu_{i\rightarrow j}) = \text{sgn}(\nu_{i\rightarrow j}) \) for all \( (i, j) \in \mathcal{E} \). When comparing two vectors, we use the partial order \( \mu \succeq \nu \) to denote \( \mu_{i\rightarrow j} \geq \nu_{i\rightarrow j} \) for all \( (i, j) \in \mathcal{E} \), and \( \mu \succeq \nu \) to denote \( \mu_{i\rightarrow j} \geq \nu_{i\rightarrow j} \) for all \( (i, j) \in \mathcal{E} \). In the sequel, \( \{\mu\} \) and \( \{\mu_{i}^{\ell}\} \) denote sequences of WMS message vectors \( \{\mu^{(\ell)} : \ell = 1, 2, \ldots \} \) and \( \{\mu_{i}^{(\ell)} : \ell = 1, 2, \ldots \} \), respectively. We extend the definition of the WMS operator in (13) to \( W_{\delta} \) for \( \beta = \frac{\delta}{d_v - 1} \). The conditions for the operator \( W_{\delta} \) to preserve the partial order of the absolute value of the WMS messages are introduced in the following lemma.

**Lemma 21.** Consider a \( (d_v, d_c) \)-regular LDPC code and a particular LLR vector \( \gamma \in \mathbb{R}^n \). Let \( \mu, \nu \in \mathbb{R}^{|\mathcal{E}|} \) be two WMS-consistent message vectors. If \( \mu \triangleright \nu \) and \( |\mu| \succeq |\nu| \geq \frac{||\gamma||}{\delta} \mathbf{1} \), then \( W_{\delta} [\mu] \succeq W_{\delta} [\nu] \) and \( W_{\delta} [\mu] = W_{\delta} [\nu] \Rightarrow \mu = \nu. \)

**Proof:** See Appendix D

When \( \beta = \frac{1}{d_v - 1} \), one may observe three kinds of trajectories of the WMS messages. They can converge to a fixed point, oscillate, or diverge to \( \pm \infty \). In this section, we are interested in the case when the sequence of WMS message vectors, \( \{\mu\} \), is divergent and WMS-consistent. We formalize this case by the following definition.
**Definition 22.** A sequence of WMS message vectors, \( \{ \mu \} \), is *divergent and consistent* if 1) for all \((i, j) \in E\), the absolute value of the WMS message, \(|\mu^{(l)}_{i \rightarrow j}|\), goes to infinity, and 2) there exists an integer \( L > 0 \) such that \( \mu^{(l)} \) is WMS-consistent whenever \( l \geq L \).

Given two positive integers \( L_1 > L_0 \), to simplify notation, we denote \( I = \{ L_0, L_0 + 1, \ldots, L_1 \} \) by \( I = [L_0, L_1] \) when it is clear from context that \( I \) contains integers. A property of the sequence of WMS message vectors, \( \{ \mu_0 \} \), is introduced in the following definition.

**Definition 23** (Block-wise monotone property). A sequence of WMS message vectors, \( \{ \mu_0 \} \), is said to have *block-wise monotone property* in interval \( I = [L_0, L_1] \) denoted by BMP\((I)\), if for all \( l \in I \), 1) \( \mu_0^{(l)} \) is WMS-consistent, 2) \( \mu_0^{(l)} \equiv \mu_0^{(L_0)} \), 3) \( |\mu_0^{(l)}| \geq \left| \frac{|\gamma_i|}{\delta} - 1 \right| \), and 4) \( |\mu_0^{(L_1)}| \geq |\mu_0^{(L_0)}| \).

In the following analysis, we show that, if there is an interval \( I_0 = [L_0, L_1] \) such that the sequence of WMS message vectors, \( \{ \mu_0 \} \), satisfies BMP\((I_0)\), then \( \{ \mu_0 \} \) also satisfies BMP\((I_k)\) for all intervals \( I_k = [L_0 + k(L_1 - L_0), L_1 + k(L_1 - L_0)] \). We first show that if \( \{ \mu_0 \} \) satisfies BMP\((I_0)\), then \( \{ \mu_0 \} \) also satisfies BMP\((I_1)\), where \( I_1 = [L_1, L_1 + (L_1 - L_0)] \).

**Lemma 24.** Let \( \gamma \in \mathbb{R}^n \) be the received LLRs, and consider the sequence of WMS message vectors \( \{ \mu_0 \} \) of a \((d_v, d_c)\)-regular LDPC code. Suppose there exists an interval \( I_0 = [L_0, L_1] \) such that \( \{ \mu_0 \} \) satisfies BMP\((I_0)\), then

\[
\mu_0^{(l' + L_1)} \equiv \mu_0^{(l' + L_0)} \quad (25)
\]

and

\[
|\mu_0^{(l' + L_1)}| \geq |\mu_0^{(l' + L_0)}| \quad (26)
\]

for all \( l' = 0, 1, \ldots, L_1 - L_0 \).

**Proof:** We prove this lemma by induction. The base case, \( l' = 0 \), is obtained since conditions 2) and 4) of BMP\((I_0)\) are satisfied.

For the inductive step, suppose that \( \mu_0^{(L_0 + l')} \equiv \mu_0^{(L_0 + l')} \) and \( |\mu_0^{(L_1 + l')}| \geq |\mu_0^{(L_0 + l')}| \). Since \( \mu_0^{(L_0 + l')} \) satisfies conditions 1) and 3) of BMP\((I_0)\), from Lemma 21 we have

\[
|\mu_0^{(L_1 + l' + 1)}| \geq |\mu_0^{(L_0 + l' + 1)}|
\]

and

\[
\mu_0^{(L_1 + l' + 1)} \equiv \mu_0^{(L_0 + l' + 1)} \equiv \mu_0^{(L_0 + l')}.
\]
Since both the base case and the inductive step are proved, we know that (25) and (26) hold for \(0 \leq \ell' \leq L_1 - L_0\).

**Corollary 25.** Let \(\gamma \in \mathbb{R}^n\) be the received LLRs, and consider the sequence of WMS message vectors, \(\{\mu_\delta\}\), of a \((d_v, d_c)\)-regular LDPC code. Suppose there exists an interval \(I_0 = [L_0, L_1]\) such that \(\{\mu_\delta\}\) satisfies BMP(I_0). Then \(\{\mu_\delta\}\) also satisfies BMP(I_1), where \(I_1 = [L_1, 2L_1 - L_0]\).

**Proof:** From Lemma 24, we know \(|\mu_\delta^{(\ell'+L_1)}| \geq |\mu_\delta^{(\ell'+L_0)}| \geq \|\gamma\|_\delta^{-1}1\) for all \(\ell' = 0, 1, \ldots, (L_1 - L_0)\). Since \(\mu_\delta^{(\ell'+L_0)}\) satisfies condition 1) of BMP(I_0), we know \(\mu_\delta^{(\ell'+L_1)}\) is also WMS-consistent. Also, (25) implies that

\[
\mu_\delta^{(\ell'+L_1)} = \mu_\delta^{(\ell'+L_0)} = \mu_\delta^{(L_1)},
\]

where the second equality in sign is by the satisfaction of condition 2) of BMP(I_0). Finally, by (26), we have

\[
\left|\mu_\delta^{(2L_1-L_0)}\right| \geq \left|\mu_\delta^{(L_1)}\right|.
\]

Therefore, we conclude that \(\{\mu_\delta\}\) also satisfies BMP(I_1) for \(I_1 = [L_1, 2L_1 - L_0]\).

Now, we extend the property to intervals \(I_k\) for all \(k \geq 0\).

**Lemma 26.** Consider the WMS algorithm with \(\beta = \frac{\delta}{d_c-1}\) on a \((d_v, d_c)\)-regular LDPC code. Let \(\gamma \in \mathbb{R}^n\) be the received LLRs. Suppose there exists an interval \(I_0 = [L_0, L_1]\) such that the sequence of WMS message vectors, \(\{\mu_\delta\}\), satisfies BMP(I_0). Then, for all \(\ell \geq L_0\), one finds that

\[
\mu_\delta^{(\ell)} = \mu_\delta^{(L_0)}
\]

and

\[
\left|\mu_\delta^{(\ell)}\right| \geq \frac{\|\gamma\|_\infty}{\delta}1.
\]

**Proof:** We first define \(\bar{L} \triangleq L_1 - L_0\) and \(L_k \triangleq L_0 + k\bar{L}\) for \(k = 0, 1, 2, \ldots\). Then, \([L_0, \infty) = \{L_0, L_0 + 1, \ldots\}\) can be written as \([L_0, \infty) = \bigcup_{k=0}^{\infty} I_k\), where \(I_k \triangleq [L_k, L_{k+1}]\). The lemma can be proved by showing that \(\{\mu_\delta\}\) satisfies BMP(I_k) for any \(k \geq 0\). We will prove this statement by induction.

The base case is obtained from the assumption when setting \(k = 0\). Next, we consider the inductive step. Suppose that \(\{\mu_\delta\}\) satisfies BMP(I_k). From Corollary 25 we know \(\{\mu_\delta\}\) also satisfies BMP(I_{k+1}). Thus, we know that \(\mu_\delta^{(\ell)}\) has BMP(I_k) property for any \(k > 0\).
In the following analysis, we show that there exist a $\delta > 0$ and an interval $I = [L_0, L_1]$ such that $\{\mu_\delta\}$ satisfies BMP($I$) when $\{\mu\}$ is divergent and consistent. We first show that, for any integer $L \geq 0$, the WMS message $\mu^{(\ell)}$ for $\ell \in [0, L]$ can be approximated by $\{\mu_\delta\}$ with $\delta$ close enough to 1.

**Lemma 27.** Consider a $(d_v, d_c)$-regular LDPC code. Given the LLR vector $\gamma \in \mathbb{R}^n$, let $\{\mu\}$ and $\{\mu_\delta\}$ be two sequences of WMS message vectors with $\beta = \frac{1}{d_v-1}$ and $\beta = \frac{\delta}{d_c-1}$, respectively. For any $\epsilon > 0$ and integer $L > 0$, there exists a $\delta \in [0, 1)$ such that $\|\mu^{(\ell)} - \mu^{(\ell)}_\delta\|_\infty < \epsilon$ for all $\ell \leq L$.

**Proof:** See Appendix E.

Given that $\{\mu\}$ is divergent and consistent, Lemma 27 implies the existence of $\delta$ and $I_0 = [L_0, L_1]$ such that $\{\mu_\delta\}$ satisfies BMP($I_0$). The choices of $\delta$ and $I_0$ are also suggested in the proof of Lemma 27.

The following lemma shows the existence of $I_0$ and $\delta$ by finding a valid pair of $I_0$ and $\delta$ such that the sequence of WMS message vectors $\{\mu_\delta\}$ satisfies BMP($I_0$), and hence, satisfies BMP($I_k$) for any $k > 0$.

**Lemma 28.** Given the received LLRs, $\gamma \in \mathbb{R}^n$, suppose that $\{\mu\}$ is divergent and consistent. There exists an interval $I_0 = [L_0, L_1]$ and a $\delta \in [0, 1)$ such that $\{\mu_\delta\}$ satisfies BMP($I_0$). By Lemma 26, this implies further that there exists an $L_0$ and $\delta$ such that

$$\left| \mu^{(\ell)}_\delta \right| \geq \frac{\|\gamma\|_\infty}{\delta} \mathbf{1}$$

and

$$\mu^{(\ell)}_\delta \leq \mu^{(L_0)}$$

whenever $\ell \geq L_0$.

**Proof:** We first introduce a valid choice of the pair of $I_0$ and $\delta$. Then, (27) and (28) are followed immediately by Lemma 26.

Since $\{\mu\}$ is divergent and consistent, it satisfies conditions 1) and 2) of Definition 22. Therefore, we can find an $L_0 > 2$ such that, for all $\ell \geq L_0$: $\mu^{(\ell)}$ is WMS-consistent; $|\mu^{(\ell)}| \geq 2\|\gamma\|_\infty \mathbf{1}$; and $\mu^{(\ell)} \leq \mu^{(L_0)}$. Similarly, we can also find an $L_1 > L_0$ such that $|\mu^{(\ell)}| \geq (\|\mu^{(L_0)}\|_\infty + 2\|\gamma\|_\infty) \mathbf{1}$ whenever $\ell > L_1$.

From Lemma 27, we can choose $\epsilon = \frac{1}{2}\|\gamma\|_\infty$ and $\delta \geq 1 - \frac{2\epsilon}{L_1 (L_1 + 1) \|\gamma\|_\infty} = 1 - \frac{1}{L_1 (L_1 + 1)}$

so that

$$\left\| \mu^{(\ell)} - \mu^{(\ell)}_\delta \right\|_\infty \leq \epsilon = \frac{1}{2}\|\gamma\|_\infty$$
for all $\ell \in [L_0, L_1]$. Note that (29) and $L_1 > L_0 > 2$ imply $\delta \geq \frac{1}{12}$. With these choices of $L_0$ and $L_1$, we have

$$
\left| \mu^{(L_{i})}_{\delta} \right| \geq \left( \| \mu^{(L_0)}_{\infty} \| + 2\| \gamma \|_{\infty} - \epsilon \right) \mathbf{1} \\
= \left( \| \mu^{(L_0)}_{\infty} \| + \frac{3}{2}\| \gamma \|_{\infty} \right) \mathbf{1} \\
\geq \left( \| \mu^{(L_0)}_{\infty} \| + \frac{1}{2}\| \gamma \|_{\infty} \right) \mathbf{1} \\
= \left( \| \mu^{(L_0)}_{\infty} \| + \epsilon \right) \mathbf{1}
$$

(31)

Since $|\mu^{(\ell)}| \geq 2\| \gamma \|_{\infty} \mathbf{1}$ for all $\ell \in [L_0, L_1]$, we know

$$
\left| \mu^{(\ell)}_{\delta} \right| \geq \left| \mu^{(\ell)} \right| - \epsilon \mathbf{1} \geq \frac{3}{2}\| \gamma \|_{\infty} \mathbf{1} \geq \frac{\| \gamma \|_{\infty}}{\delta} \mathbf{1}
$$

(32)

for all $\ell \in [L_0, L_1]$. Also by the fact that $|\mu^{(\ell)}| \geq 2\| \gamma \|_{\infty} \mathbf{1}$ and $\mu^{(\ell)} \preceq \mu^{(L_0)}$, we know that

$$
\mu^{(\ell)}_{\delta} \preceq \mu^{(\ell)} \preceq \mu^{(L_0)} \preceq \mu^{(L_0)}_{\delta}
$$

(33)

for all $\ell \in I_0$. Since $\mu^{(L_0)}$ is WMS-consistent, (33) implies that $\mu^{(\ell)}_{\delta}$ is WMS-consistent for all $\ell \in I_0$ as well. By (31)–(33) and the fact that $\mu^{(\ell)}_{\delta}$ is WMS-consistent for all $\ell \in I_0$, we conclude that $\{\mu^{(\ell)}_{\delta}\}$ satisfies BMP($I_0$). From Lemma 26 we obtain (27) and (28) directly.

Theorem 29. Consider a $(d_v, d_c)$-regular LDPC code and a particular LLR vector $\gamma \in \mathbb{R}^n$. If the WMS algorithm diverges (i.e., the messages tend to $\pm \infty$) to consistent messages for $\beta = \frac{1}{d_v-1}$, then there is a $\delta \in [0, 1)$ such that it also converges to consistent messages whose hard decisions give the same codeword as the WMS algorithm for $\beta = \frac{\delta}{d_v-1}$. In this case, the codeword is the LP optimal and, hence, ML codeword.

Proof: From Lemma 28 we have shown that there exist a $L_0 > 0$ and a $0 \leq \delta < 1$ such that $\mu^{(\ell)}_{\delta} \preceq \mu^{(\ell)} \preceq \mu^{(L_0)}$ for all $\ell \geq L_0$. Since $\frac{\delta}{d_v-1} < \frac{1}{d_v-1}$, we know the messages will converge to a fixed point $\mu^{*}_{\delta}$ and $\mu^{*}_{\delta} \preceq \mu^{(L_0)}$. Since $\mu^{(L_0)}$ is WMS-consistent, the converged message vector $\mu^{*}_{\delta}$ is also WMS-consistent. Hence, for all $(i, j) \in E$

$$
\text{sgn} \left( \gamma_i + \beta \sum_{j \in N(i)} \mu^{*}_{\delta,i \leftarrow j} \right) = \text{sgn} \left( \mu^{*}_{\delta,i \leftarrow j} \right)
$$

$$
= \text{sgn} \left( \mu^{(L_0)}_{i \leftarrow j} \right) = \text{sgn} \left( \gamma_i + \frac{1}{d_v - 1} \sum_{j \in N(i)} \mu^{(L_0)}_{i \leftarrow j} \right).
$$
For any $i \in \mathcal{V}_L$, the hard decision $x_{\delta,i}^*$ with $\beta = \frac{\delta}{d_v - 1}$ is

$$x_{\delta,i}^* = \frac{1}{2} \left( 1 - \text{sgn} \left( \gamma_i + \beta \sum_{j \in N(i)} \mu_{i \rightarrow j}^* \right) \right) = \frac{1}{2} \left( 1 - \text{sgn} \left( \gamma_i + \frac{1}{d_v - 1} \sum_{j \in N(i)} \mu_{i \rightarrow j}^{(L_0)} \right) \right) = x_i^{(L_0)}.$$

From Theorem [39] we know that $x_{\delta}^*$ is LP and ML optimal. Therefore, the hard decision vector $x^{(L_0)}$ is also an LP and ML optimal codeword.

Remark 30. In this paper, we considered the WMS algorithm as a DP problem with discount factor $\beta (d_v - 1) \leq 1$. When $\beta = \frac{1}{d_v - 1}$ and the sequence of WMS message vectors $\{\mu\}$ is divergent and consistent, the WMS update is equivalent to an Markov decision process (MDP) problem with discount factor 1. Theorem [29] essentially states that WMS decoding always has the natural analog of a Blackwell optimal policy if $\{\mu\}$ is divergent and consistent according to Definition [22].

A. Connections with LP Thresholds

In this subsection, we connect the LP threshold estimation with both the WMS algorithm and the DE type analysis in [16], [17]. We have shown that when the WMS algorithm with $\beta < \frac{1}{d_v - 1}$ converges to a set of consistent messages, the WMS algorithm returns a codeword which is LP optimal. Similarly, when the WMS algorithm with $\beta = \frac{1}{d_v - 1}$ satisfies conditions 1) and 2) of Definition [22], the WMS algorithm also returns a codeword which is LP optimal. If the following conjecture is true, we can conclude that the threshold of the WMS algorithm with $\beta = \frac{1}{d_v - 1}$ gives a lower bound for the threshold of LP decoding.

Conjecture 31. Consider the WMS decoding of $(d_v, d_c)$-regular LDPC codes with girth $\Omega (\log n)$ over a BSC with cross-over probability $p$ and let $p^*$ be the bit-error rate threshold for the WMS decoding with $\beta = \frac{1}{d_v - 1}$. Then, the WMS decoding diverges to consistent messages with high probability for all $p < p^*$.

Remark 32. DE gives automatically that almost all messages diverge to consistent values (i.e., a BER threshold). Conjecture [31] is that $p^*$ is also a word-error rate (WER) threshold. Conjecture [31] has been tested via simulation, and we are currently pursuing a rigorous proof.
Example 33. Consider a \((3, 6)\)-regular LDPC code over a BSC. From a DE analysis of the WMS algorithm (i.e., not the DE for local optimality proposed in [16]) with \(\beta = 1/2\), one finds that the WMS algorithm will decode correctly when \(p \leq 0.055\).

Remark 34. In the Example 33, the LP threshold lower bound of 0.055 matches the best possible bound using techniques from [16]. The main improvement over [16] is that our analysis (under the conjectures) holds pointwise for any received sequence.

V. Numerical Results

The word error rate (WER) for the WMS algorithms and the probability of not converging to a set of consistent messages are shown in Figure 1. The solid lines are the WER of the WMS algorithm, and the dashed lines are the probability of not WMS-consistent. The simulation is conducted over a \((3, 6)\)-regular LDPC code ensemble with \(n = 10^4\). Two weight factors, \(\beta = 0.49\) and \(\beta = 0.5\), are considered, and 500 iterations are performed in decoding one codeword. Both the BSC and BIAWGNC are tested. As shown in Figure 1 when \(\beta = 0.49\), the WMS algorithm may converge to a set of not WMS-consistent messages even though the codeword is successfully decoded. However, when \(\beta = 0.5\), those two probabilities become nearly identical.

To get the lower bound of the LP decoding threshold, a DE-type analysis is employed in [16] and [17]. The lower bound provided by the DE-type analysis depends on \(\beta\) though and is plotted in Figure 2. It is worth noting that according to our simulation result, the best lower bounds, in all cases, are obtained when \(\beta = \frac{1}{d_v - 1}\), and that there is no threshold effect when \(\beta < \frac{1}{d_v - 1}\). The threshold effect does not occur because the density of the correlation between the best skinny trees and the channel output in [16], [17] converges to a fixed point instead of diverging to \(\pm \infty\).

The comparisons of the WER performance between the WMS algorithm and the TRMP algorithm are shown in Figure 3. For any strictly positive pairwise Markov random field (MRF) with binary variables, it has been shown that the fixed point of the TRMP algorithm always specifies an optimal dual solution [10], [20]. The TRMP message update rules in logarithm domain is

\[
\nu_{i \rightarrow j}^{(\ell+1)} = \gamma_i + \rho \sum_{k \in N(i) \setminus j} \nu_{i \leftarrow k}^{(\ell)} - (1 - \rho) \nu_{i \leftarrow j}^{(\ell)},
\]

\[
\nu_{i \leftarrow j}^{(\ell+1)} = \rho \left( \prod_{m \in N(j) \setminus i} \sgn \left( \nu_{m \rightarrow j}^{(\ell)} \right) \right) \min_{m' \in N(j) \setminus i} \left| \nu_{m' \rightarrow j}^{(\ell)} - (1 - \rho) \nu_{i \leftarrow j}^{(\ell)} \right|.
\]
Figure 1. The WER (solid lines) of the WMS algorithm for (3, 6)-regular LDPC code and the probability of converging to inconsistent messages (dashed lines).

where $\rho \leq 1$ is the edge appearance probability. An uniform edge appearance probability $\rho = \frac{n(1+d_c/d_v)-1}{|E|}$ is employed in our simulation. One can notice that these update rules are similar to the WMS algorithms. Although, the factor graph for LDPC code is not strictly positive, the optimality of the TRMP hard decisions is observed in a numerical simulation of a (3, 4)-regular LDPC code with $n = 12$. Thus, we take the TRMP algorithm into consideration, and compare its WER performance with the WER performance of the WMS algorithms.

In this comparison, a (3, 6)-regular LDPC codes over BSC is considered, and the codeword length for both algorithms is $n = 10^4$. Three weight factors for the WMS algorithm are tested: $\beta = 0.5$, which is discussed in this paper; $\beta = 0.8$, which has been shown to have best performance by DE analysis \cite{18}; and $\beta = 1$, which is equivalent to the conventional min-sum algorithm for LDPC codes. All WMS algorithms perform 100 iterations in decoding a codeword. In TRMP algorithm, two simulations with 100
Figure 2. The lower bound of the LP decoding threshold for (3, 6), (4, 8) and (5, 10)-regular LDPC codes over BIAWGNC and BSC.

iterations and 1000 iterations, respectively, for decoding a codeword are conducted. As shown in Figure 3, the WER performance of the TRMP algorithm with 1000 iterations is close to the WMS algorithm with $\beta = 1$. However, if the TRMP algorithm only performs 100 iterations in decoding each codeword, it becomes close to the WMS algorithm with $\beta = 0.5$. The performance loss of the TRMP algorithm with 100 iterations is caused by the insufficient number of iterations. Since the TRMP algorithm is not close enough to the converged point, the corresponding hard decision bits are not reliable. Although TRMP algorithm over binary alphabet has been shown LP optimal when the algorithm converges, finding the noise threshold of the TRMP algorithm is still an open problem.
Figure 3. WER performance comparisons for a (3, 6)-regular LDPC code over the BSC.

VI. CONCLUSIONS AND FUTURE WORK

For \((d_v, d_c)\)-regular LDPC codes, both the attenuated max-product (AMP) algorithm and the weighted min-sum (WMS) algorithm are studied. By slightly modifying the objective function of the original AMP problem in (3) to an equivalent problem in (8), we show that the AMP messages will converge to a fixed point when \(\beta < \frac{1}{(d_v - 1)(d_c - 1)}\). Further, a set of sufficient conditions (AMP-consistency) for testing the optimality of the AMP solutions is proposed. With the modified AMP problem in (8), we show the LP and ML optimality of the AMP solution by a simple proof if \(\beta < \frac{1}{(d_v - 1)(d_c - 1)}\) and the fixed point is AMP-consistent.

Similarly, when the weight factor \(\beta < \frac{1}{d_v - 1}\), we show that the WMS algorithm converges to a unique fixed point. We also introduce the sufficient conditions (WMS-consistency) for the hard decisions of the WMS algorithm to be a valid codeword. By employing the construction of a dual feasible point of the LP decoding (Problem-P) in [15], we show that if \(\beta < \frac{1}{d_v - 1}\) and the WMS algorithm converges to a
consistent codeword, we can simplify the construction by using the converged messages. Also, we show that the dual feasible point obtained by the converged messages is an optimal dual feasible point, and the corresponding hard decisions are the LP optimum as well as the ML solution. Based on the analysis of the WMS algorithm with $\beta < \frac{1}{d_v-1}$, the optimality of the WMS algorithm with $\beta = \frac{1}{d_v-1}$ is also discussed. When the WMS messages with $\beta = \frac{1}{d_v-1}$ satisfy the consistency conditions and diverge to $\pm \infty$, we show that the hard decisions is ML optimum as well. This result can be seen as the natural completion of the work initiated by Koetter and Frey in [7]. Also, our results have interesting connections with the results of [16] because their best LP thresholds also occur when $\beta = \frac{1}{d_v-1}$ according to DE analysis. For weight factors $\beta > \frac{1}{d_v-1}$, we provide a counterexample which shows that it is not always possible to provide ML certificates for WMS decoding.

In regards to future work, the most interesting open question is whether connections between LP decoding and WMS decoding can be extended beyond $\beta = \frac{1}{d_v-1}$. In [18], Chen et al. studied the optimal attenuation factor for the WMS algorithm. For example, the best $\beta$ for the $(3,6)$-regular LDPC code on the BSC is $\beta = 0.8$, and the corresponding threshold is $p = 0.083$. DE also shows that any extension beyond $\beta = \frac{1}{d_v-1}$ will provide an improved lower bound on the LP threshold. Moreover, the construction of an optimal dual-feasible point for the LP decoding on an irregular LDPC code using WMS messages is still unclear to us. Let $d_{v,i}$ be the degree of the $i$th bit. With the construction proposed in this paper, we need $\beta_i = \beta < \min_{i' \in \mathcal{V}_L} \left\{ \frac{1}{d_{v,i'}-1} \right\}$ for all $i \in \mathcal{V}_L$ to ensure the convergence of WMS messages and the optimality of the corresponding dual-feasible point. However, there exists no threshold for the WMS algorithm with this choice of $\beta_i$. Therefore, a general weighting strategy and the corresponding construction of the optimal dual-feasible point for irregular LDPC codes is still an open problem. Since the irregular LDPC code has been proved to be capacity-approaching in [4], we expect that the irregular LDPC code with general weighting scheme can improve current estimate of the noise threshold for the LP decoding over a rate-$\frac{1}{2}$ LDPC code.

APPENDIX A

PROOF OF LEMMA 3

Proof: Let $\ell, m \leq n$ be the integers such that $f_{\ell} = \max_i f_i$ and $g_m = \max_i g_i$. If $f_{\ell} \geq g_m$, it can be shown that $f_{\ell} - g_i \geq 0$ for all $i = 1, 2, \ldots, n$. Thus, it follows that

$$\max_i |f_i - g_i| \geq |f_{\ell} - g_\ell| = f_{\ell} - g_\ell \geq f_{\ell} - g_m = |f_{\ell} - g_m|.$$
On the other hand, if \( f_\ell \leq g_m \), we still can have the same inequality by

\[
\max_i |f_i - g_i| \geq |f_m - g_m| = g_m - f_m \geq g_m - f_\ell = |f_\ell - g_m|.
\]

Therefore, we obtain (16).

APPENDIX B

PROOF OF LEMMA [7]

Proof: By the definition of the DP value function in (9), we have

\[ \sum_{(i,j) \in \mathcal{E}} \mu^*_{i \rightarrow j} (x_{i,j}) = \sum_{(i,j) \in \mathcal{E}} (1 - x_{i,j}) \gamma_i + \beta \sum_{(i,j) \in \mathcal{E}} \max_{k \in N(i) \setminus j} \sum_{m \in \mathcal{N}(k) \setminus i} \mu^*_{m \rightarrow k} (w_m), \tag{34} \]

where \( \mathcal{S}_{k,i}(x_{i,j}) \) is defined in (6). Since \( x^*_{i,j} \) maximizes \( \mu^*_{i \rightarrow j}(x) \), the inequality can be obtained by simply replacing \( w_m \) in (34) with \( x^*_{m,k} \). Thus, we have

\[
\sum_{(i,j) \in \mathcal{E}} \mu^*_{i \rightarrow j} (x^*_{i,j}) \leq \sum_{(i,j) \in \mathcal{E}} (1 - x^*_{i,j}) \gamma_i + \beta \sum_{(i,j) \in \mathcal{E}} \max_{k \in N(i) \setminus j} \sum_{m \in \mathcal{N}(k) \setminus i} \mu^*_{m \rightarrow k} (x^*_{m,k})
\]

\[
= \sum_{(i,j) \in \mathcal{E}} (1 - x^*_{i,j}) \gamma_i + \beta (d_v - 1) (d_c - 1) \sum_{(i,j) \in \mathcal{E}} \mu^*_{i \rightarrow j} (x^*_{i,j}).
\]

To show the equality, by substituting \( x^*_{i,j} \) into (34), we have

\[
\sum_{(i,j) \in \mathcal{E}} \mu^*_{i \rightarrow j} (x^*_{i,j}) = \sum_{(i,j) \in \mathcal{E}} (1 - x^*_{i,j}) \gamma_i + \beta \sum_{(i,j) \in \mathcal{E}} \max_{k \in N(i) \setminus j} \sum_{m \in \mathcal{N}(k) \setminus i} \mu^*_{m \rightarrow k} (w_m). \tag{35}
\]

Since \( \{x^*_{i,j}\} \) is AMP-consistent, there exists a vector \( \mathbf{x}^* \in \mathcal{C} \) such that \( x^*_{i,j} = x^*_{i,j} \) for all \( i \in \mathcal{V}_L \) and \( j \in N(i) \). By the fact that \( \mathbf{x}^* \in \mathcal{S}_{k,i}(x^*_{i,j}) \), the last term in equation (35) is equal to

\[
\beta \sum_{(i,j) \in \mathcal{E}, k \in N(i) \setminus j, m \in \mathcal{N}(k) \setminus i} \mu^*_{m \rightarrow k} (x^*_{m,k}).
\]

Therefore, we obtain the equality.

APPENDIX C

PROOF OF LEMMA [12]

Proof: Since \( \prod_{m \in \mathcal{N}(k) \setminus i} \text{sgn}(\mu_{m \rightarrow k}) \text{sgn}(\nu_{m \rightarrow k}) \) can be \( \pm 1 \), we must show that

\[
\max_{m \in \mathcal{N}(k) \setminus i} |\mu_{m \rightarrow k} - \nu_{m \rightarrow k}| \geq \left| \min_{m \in \mathcal{N}(k) \setminus i} |\mu_{m \rightarrow k}| - \min_{m \in \mathcal{N}(k) \setminus i} |\nu_{m \rightarrow k}| \right|, \tag{36}
\]
when all $\mu_{m \rightarrow k}, \nu_{m \rightarrow k}$ signs match on $m \in N(k) \setminus i$, and

$$\max_{m \in N(k) \setminus i} |\mu_{m \rightarrow k} - \nu_{m \rightarrow k}| \geq \left| \min_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}| + \min_{m \in N(k) \setminus i} |\nu_{m \rightarrow k}| \right|,$$

(37)

when some signs differ.

To show (36), define the following indices

$$m_1 \triangleq \arg \min_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}|,$$

$$m_2 \triangleq \arg \min_{m \in N(k) \setminus i} |\nu_{m \rightarrow k}|,$$

and

$$m^* \triangleq \arg \max_{m \in N(k) \setminus i} |\mu_{m \rightarrow k} - \nu_{m \rightarrow k}|.$$

Notice that

$$|\mu_{m^* \rightarrow k} - \nu_{m^* \rightarrow k}| \geq \max_{m \in N(k) \setminus i} \left| |\mu_{m \rightarrow k}| - |\nu_{m \rightarrow k}| \right| = \max_{m \in N(k) \setminus i} \left| |\nu_{m \rightarrow k}| - |\mu_{m \rightarrow k}| \right|.$$

Consider the case when $|\mu_{m_1 \rightarrow k}| \geq |\nu_{m_2 \rightarrow k}|$. Since $|\mu_{m_2 \rightarrow k}| \geq |\mu_{m_1 \rightarrow k}| \geq |\nu_{m_2 \rightarrow k}|$, it follows that

$$|\mu_{m^* \rightarrow k} - \nu_{m^* \rightarrow k}| \geq \max_{m \in N(k) \setminus i} \left| |\mu_{m \rightarrow k}| - |\nu_{m \rightarrow k}| \right| \geq \left| |\mu_{m_2 \rightarrow k}| - |\nu_{m_2 \rightarrow k}| \right| \geq \left| |\mu_{m_1 \rightarrow k}| - |\nu_{m_2 \rightarrow k}| \right|.$$

(38)

When $|\mu_{m_1 \rightarrow k}| \leq |\nu_{m_2 \rightarrow k}|$, we know $|\mu_{m_1 \rightarrow k}| \leq |\nu_{m_2 \rightarrow k}| \leq |\nu_{m_1 \rightarrow k}|$. It can be shown that

$$\max_{m \in N(k) \setminus i} \left| |\mu_{m \rightarrow k}| - |\nu_{m \rightarrow k}| \right| \geq \left| |\mu_{m_1 \rightarrow k}| - |\mu_{m_1 \rightarrow k}| \right| \geq \left| |\nu_{m_2 \rightarrow k}| - |\mu_{m_1 \rightarrow k}| \right| \geq \left| |\mu_{m_1 \rightarrow k}| - |\nu_{m_2 \rightarrow k}| \right|,$$

(39)

and combining the results in (38) and (39) implies (36).

To show (37), let $M = \{m \in N(k) \setminus i : \mu_{m \rightarrow k} \nu_{m \rightarrow k} < 0\}$ be the set of indices such that $\mu_{m \rightarrow k}$ and $\nu_{m \rightarrow k}$ have different signs. Notice that
\[
\max_{m \in N(k) \setminus i} |\mu_{m \rightarrow k} - \nu_{m \rightarrow k}| \geq \max_{m \in M} |\mu_{m \rightarrow k} - \nu_{m \rightarrow k}|
\]
\[
\geq \max_{m \in M} (|\mu_{m \rightarrow k}| + |\nu_{m \rightarrow k}|)
\]
\[
\geq \left| \min_{m \in M} |\mu_{m \rightarrow k}| + \min_{m \in M} |\nu_{m \rightarrow k}| \right|
\]
\[
\geq \left| \min_{m \in N(k) \setminus i} |\mu_{m \rightarrow k}| + \min_{m \in N(k) \setminus i} |\nu_{m \rightarrow k}| \right|.
\]

This completes the proof. \[\blacksquare\]

**APPENDIX D**

**PROOF OF LEMMA 21**

*Proof:* Let \(\mu' \triangleq W_\delta[\mu]\) and \(\nu' \triangleq W_\delta[\nu]\). One can compute the sign of the check-to-bit messages for each edge \((i, j) \in E\) as \(\operatorname{sgn}(\mu_{i \leftarrow j}) = \prod_{m \in N(j) \setminus i} \operatorname{sgn}(\mu_{m \rightarrow j})\) and \(\operatorname{sgn}(\nu_{i \leftarrow j}) = \prod_{m \in N(j) \setminus i} \operatorname{sgn}(\nu_{m \rightarrow j})\). Using this and \(\mu \triangleq \nu\), it follows that

\[
\operatorname{sgn}(\mu_{i \leftarrow j}) = \operatorname{sgn}(\nu_{i \leftarrow j})
\]

(40)

for all \((i, j) \in E\).

Since \(\mu, \nu\) both satisfy the consistency conditions, we know that \(\operatorname{sgn}(\mu_{i \leftarrow j}) = \operatorname{sgn}(\mu_{i \leftarrow j}')\) and \(\operatorname{sgn}(\nu_{i \leftarrow j}) = \operatorname{sgn}(\nu_{i \leftarrow j}')\) for all \(j, j' \in N(i)\). Thus, for each \((i, j) \in E\), \(\mu'_{i \rightarrow j}\) and \(\nu'_{i \rightarrow j}\) can be expressed as

\[
\mu'_{i \rightarrow j} = \operatorname{sgn}(\mu_{i \leftarrow j}) \left( \operatorname{sgn}(\mu_{i \leftarrow j}) \gamma_i + \frac{\delta}{d_v - 1} \sum_{k \in N(i) \setminus j} \min_{m' \in N(k) \setminus i} |\mu_{m' \rightarrow k}| \right)
\]

(41)

and

\[
\nu'_{i \rightarrow j} = \operatorname{sgn}(\nu_{i \leftarrow j}) \left( \operatorname{sgn}(\nu_{i \leftarrow j}) \gamma_i + \frac{\delta}{d_v - 1} \sum_{k \in N(i) \setminus j} \min_{m' \in N(k) \setminus i} |\nu_{m' \rightarrow k}| \right).
\]

(42)

Since \(|\nu| \geq \frac{||\gamma||_\infty}{\delta} 1\), we have

\[
\operatorname{sgn}(\nu_{i \leftarrow j}) \gamma_i + \frac{\delta}{d_v - 1} \sum_{k \in N(i) \setminus j} \min_{m' \in N(k) \setminus i} |\nu_{m' \rightarrow k}|
\]

\[
\geq \operatorname{sgn}(\nu_{i \leftarrow j}) \gamma_i + ||\gamma||_\infty \geq 0.
\]

(43)

Hence,

\[
|\nu'_{i \rightarrow j}| = \operatorname{sgn}(\nu_{i \leftarrow j}) \gamma_i + \frac{\delta}{d_v - 1} \sum_{k \in N(i) \setminus j} \min_{m' \in N(k) \setminus i} |\nu_{m' \rightarrow k}|
\]
and similarly,
\[ |\mu'_{i \rightarrow j}| = \text{sgn}(\mu_{i \rightarrow j}) \gamma_i + \frac{\delta}{d_v - 1} \sum_{k \in N(i) \backslash j} \min_{m' \in N(k) \backslash i} |\mu_{m' \rightarrow k}|. \]

By \(|\mu| \geq |\nu|\) and (40), we have \(|\mu'| \geq |\nu'|\).

Moreover, from (41), (42) and (43), the signs of \(\mu'_{i \rightarrow j}\) and \(\nu'_{i \rightarrow j}\) satisfy \(\text{sgn}(\nu'_{i \rightarrow j}) = \text{sgn}(\nu_{i \rightarrow j})\) and \(\text{sgn}(\mu'_{i \rightarrow j}) = \text{sgn}(\mu_{i \rightarrow j})\). By the consistency property of \(\mu\) and \(\nu\), we know \(\text{sgn}(\nu'_{i \rightarrow j}) = \text{sgn}(\nu_{i \rightarrow j}) = \text{sgn}(\nu'_{i \rightarrow j}) = \text{sgn}(\nu_{i \rightarrow j})\) for all \((i, j) \in \mathcal{E}\). This concludes the proof.

\section*{Appendix E}

\textbf{Proof of Lemma 27}

\textbf{Proof:} From (11), the absolute value of the difference \(\mu^{(\ell)}_{i \rightarrow j} - \mu^{(\ell)}_{\delta,i \rightarrow j}\) in the \(\ell\)th iteration can be written as
\[ |\mu^{(\ell)}_{i \rightarrow j} - \mu^{(\ell)}_{\delta,i \rightarrow j}| = \left| \frac{1}{d_v - 1} \sum_{k \in N(i) \backslash j} \mu^{(\ell-1)}_{i \rightarrow k} - \frac{\delta}{d_v - 1} \sum_{k' \in N(i) \backslash j} \mu^{(\ell-1)}_{\delta,i \rightarrow k'} \right|. \] (44)

By triangle inequality, (44) is upper bounded by
\[ \frac{\delta}{d_v - 1} \sum_{k \in N(i) \backslash j} |\mu^{(\ell-1)}_{i \rightarrow k} - \mu^{(\ell-1)}_{\delta,i \rightarrow k}| + \frac{1 - \delta}{d_v - 1} \sum_{k' \in N(i) \backslash j} |\mu^{(\ell-1)}_{i \rightarrow k'}|. \]

From Lemma 12 and 12, we know \(|\mu^{(\ell-1)}_{i \rightarrow k} - \mu^{(\ell-1)}_{\delta,i \rightarrow k}| \leq \max_{m \in N(k) \backslash i} |\mu^{(\ell-1)}_{m \rightarrow k} - \mu^{(\ell-1)}_{\delta,m \rightarrow k}|\). Also, by the fact that \(|\mu^{(\ell-1)}_{i \rightarrow k'}| = \min_{m \in N(k') \backslash i} |\mu^{(\ell-1)}_{m \rightarrow k'}|\), we can further upper bound (44) by
\[ \frac{\delta}{d_v - 1} \sum_{k \in N(i) \backslash j} \max_{m \in N(k) \backslash i} |\mu^{(\ell-1)}_{m \rightarrow k} - \mu^{(\ell-1)}_{\delta,m \rightarrow k}| \]
\[ + \frac{1 - \delta}{d_v - 1} \sum_{k' \in N(i) \backslash j} \min_{m \in N(k') \backslash i} |\mu^{(\ell-1)}_{m \rightarrow k'}|. \]

Since \(|\mu^{(\ell-1)}_{i \rightarrow j} - \mu^{(\ell-1)}_{\delta,i \rightarrow j}| \leq \|\mu^{(\ell-1)} - \mu^{(\ell-1)}\|_\infty\) and \(|\mu^{(\ell-1)}_{i \rightarrow j}| \leq \|\gamma\|_\infty\) for all \((i, j) \in \mathcal{E}\), we have
\[ |\mu^{(\ell)}_{i \rightarrow j} - \mu^{(\ell)}_{\delta,i \rightarrow j}| \leq \frac{\delta}{d_v - 1} \sum_{k \in N(i) \backslash j} \|\mu^{(\ell-1)}_{i \rightarrow j} - \mu^{(\ell-1)}_{\delta,i \rightarrow j}\|_\infty \]
\[ + \frac{1 - \delta}{d_v - 1} \sum_{k' \in N(i) \backslash j} \ell \|\gamma\|_\infty \]
\[ \leq \|\mu^{(\ell-1)} - \mu^{(\ell-1)}_{\delta}\|_\infty + (1 - \delta)\ell \|\gamma\|_\infty. \] (45)

Since the RHS of (45) is a constant with respect to \((i, j) \in \mathcal{E}\), one gets the recursive upper bound
\[ \|\mu^{(\ell)} - \mu^{(\ell)}_{\delta}\|_\infty \leq \|\mu^{(\ell-1)} - \mu^{(\ell-1)}_{\delta}\|_\infty + (1 - \delta)\ell \|\gamma\|_\infty. \] (46)
Note that $|\mu_{i \rightarrow j}^{(0)} - \mu_{\tilde{h}, i \rightarrow j}^{(0)}| = 0$. For a given $\ell \leq L$, we can apply (46) recursively, and have
\[
\left\| \mu^{(\ell)} - \mu_{\tilde{\delta}}^{(\ell)} \right\|_\infty < (1 - \delta) \frac{\ell (\ell + 1)}{2} \| \gamma \|_\infty \leq (1 - \delta) L \frac{L (L + 1)}{2} \| \gamma \|_\infty,
\]
for all $\ell \leq L$. Therefore, for any fixed $\epsilon > 0$, if we choose
\[
\delta \geq 1 - \frac{2\epsilon}{L (L + 1) \| \gamma \|_\infty},
\]
then $|\mu_{i \rightarrow j}^{(\ell)} - \mu_{\tilde{h}, i \rightarrow j}^{(\ell)}| \leq \| \mu^{(\ell)} - \mu_{\tilde{\delta}}^{(\ell)} \|_\infty < \epsilon$ for all $\ell \leq L$.

\section*{Appendix F}
\textbf{Extensions of the Work in [16]}

In this appendix, we briefly recall the main idea and statement in our earlier work in [19], and provide detail proves of lemmas, which were omitted in [19]. We extend the lemmas and theorems in [16] to the case when the depth of the computation tree exceeds $\frac{1}{4} \text{girth}(G)$. With these extended results, another proof of the conclusion drawn in Section II-B is obtained.

Since a computation tree with depth greater than $\frac{1}{4} \text{girth}(G)$ is considered in this section, we generalize the definition in Section II-B as follows. Let $T_{i_0}^{2T} = (\mathcal{I} \cup \mathcal{J}, \mathcal{E}')$ be a depth-$2T$ computation tree and rooted at $i_0 \in V_L$, where $\mathcal{I}$ and $\mathcal{J}$ are the set of variable nodes and the set of check nodes in $T_{i_0}^{2L}$, respectively, and $T \geq \frac{1}{4} \text{girth}(G)$. Let $i'$ and $j'$ denote a variable node and a check node in $T_{i_0}^{2T}$, respectively. We say that $i'$ is associated with the bit $i \in V_L$ in $G$ (denoted $i' \sim i$) if $i'$ is a copy of $i$. Similarly, $j' \sim j$ denotes that $j' \in \mathcal{J}$ is a copy of $j \in V_R$. Moreover, we define two projections $\eta : \mathcal{I} \rightarrow V_L$ and $\theta : \mathcal{J} \rightarrow V_R$ by $\eta(i') = \{ i \in V_L : i' \sim i \}$ and $\theta(j') = \{ j \in V_R : j' \sim j \}$.

At first, we generalize the definitions from [5] and [16] Definition 1 as follows.

\begin{definition}
Consider a computation tree $T_{i_0}^{2T} = (\mathcal{I} \cup \mathcal{J}, \mathcal{E}')$ of depth $2T \geq \frac{1}{4} \text{girth}(G)$ and rooted at $i_0$. A bit assignment $u \in \{0, 1\}^{\mathcal{I}}$ on $T_{i_0}^{2T}$ is a generalized valid deviation of depth $T$ at $i_0 \in V_L$ or, in short, a generalized $T$-local deviation if, for every check node $j \in T_{i_0}^{2T}$, at most two neighbor bits are assigned the value 1. Note that a generalized minimal $T$-local deviation at $i_0$ can be seen as a subtree of $T_{i_0}^{2T}$ of depth $2T$ rooted at $i_0$, where every variable node has full degree and every check node has degree 2. Such a tree is referred as a skinny tree. If $\varpi = (\varpi_0, \ldots, \varpi_T) \in [0, 1]^T$ is a weight vector and $u$ is a generalized minimal $T$-local deviation at $i_0$, then $u(\varpi)$ denotes the $\varpi$-weighted
\end{definition}
For any $\varpi$-weighted deviation $u^{(\varpi)}$ on $T_{i_0}^{2I}$, let the projection of $u^{(\varpi)}$ onto the code bit $i \in V_L$ be

$$
\pi_i\left(u^{(\varpi)}\right) = \sum_{t=0}^{T} \varpi_t \sum_{m \in N(i_0, 2t) : m \sim i} u_m.
$$

Likewise, we let $\pi(u^{(\varpi)})$ represent the vector whose elements are $\pi_i\left(u^{(\varpi)}\right)$ for $i \in V_L$. The weights are chosen to be $\varpi_t = \beta^t$ for some $\beta \in [0, 1]$.

To extend the results of [16] to the computation trees of depth $I \to \infty$, we utilize the following fact that, for each $i_0 \in V_L$, the WMS algorithm computes the best assignment, $\tilde{x}_{i_0}$, for the root of $T_{i_0}^{2I}$, and there is a corresponding best assignment $\tilde{x}$ for the tree $T_{i_0}^{2I}$. In the following lemma, a weighted correlation between $\tilde{x}$ and a generalized minimal $I$-local deviation is introduced. Since $\tilde{x}$ is the best assignment, it can be shown that the weighted correlation is positive when the number of iterations is large enough.

**Lemma 36.** Given the LLR vector $\gamma \in \mathbb{R}^n$, let the assignment $\tilde{x}$ for the computation tree $T_{i_0}^{2I}$, computed by the WMS decoding with $\beta < \frac{1}{d_v-1}$, be unique (i.e., there are no ties) after $I \to \infty$ iterations. Let $\tilde{x}$ be the corresponding assignment for $T_{i_0}^{2I}$. For any generalized minimal $I$-local deviation, $\tilde{u}$, rooted at $i_0$ and any $T \ll I$, let the $T$-level weighted correlation be

$$
U_{i_0}^T(\tilde{x}, \tilde{u}) \triangleq \sum_{i=1}^{n} \sum_{t=0}^{T} \beta^t \sum_{m \in N(i_0, 2t) : m \sim i} (-1)^m \tilde{u}_m \gamma_i,
$$

where $N(i_0, \ell)$ is the set of vertices in the $\ell$th level of $T_{i_0}^{2I}$. Then, there exists a $T_0 < \infty$ such that $U_{i_0}^T(\tilde{x}, \tilde{u}) > 0$ for all $T \geq T_0$ and for all $\tilde{u}$.

**Proof:** Since $\tilde{x}$ is the optimal WMS assignment for the computation tree $T_{i_0}^{2I}$ after $I$ iterations, there exists an $\epsilon > 0$ such that, for all generalized minimal $I$-local deviations $\tilde{u}$, we have
Since the computation tree.

Remark 37. Let $\tilde{x}$ and $\tilde{u}$ be as defined in Lemma 36 and let $T \geq T_0$. Since $U_{i_0}^T(\tilde{x}, \tilde{u}) > 0$, it follows that $V_{i_0}^T(\tilde{x} \oplus \tilde{u}) = V_{i_0}^T(\tilde{x}) + U_{i_0}^T(\tilde{x}, \tilde{u}) > V_{i_0}^T(\tilde{x})$ for all $\tilde{u}$. This observation implies that, when $\beta < \frac{1}{d_v - 1}$ and the number of iterations is large, the binary assignments of the leaf nodes are asymptotically irrelevant to the assignment of $\tilde{x}_{i_0}$.

The following extends the key result [16, Lemma 4] to our generalized minimal local deviations on the computation tree.
**Lemma 38.** Let $\mathcal{P}$ be the fundamental polytope of an LDPC, and $z \in \mathcal{P}$ be a LP solution of a bit-regular code. Consider the set of depth-1 computation trees rooted at all non-zero variable nodes. For these trees, there exists a distribution over generalized minimal local deviations such that the expected value, when projected onto the original Tanner graph, is proportional to the LP solution $z$.

**Proof:** This fact was first observed in [21, Remark 22]. See Appendix G for a proof based on extending the proof of [16, Lemma 4].

The following theorem shows that if the WMS messages converge to a WMS-consistent fixed point, then the hard decision bits of the WMS algorithm give a codeword that is both LP optimal and ML.

**Theorem 39.** For a given the LLR vector $\gamma \in \mathbb{R}^n$ and a weight $0 \leq \beta < \frac{1}{d_v-1}$, suppose the WMS algorithm converges to a WMS-consistent fixed point. If the hard decision bits $\hat{x}$ are unique (i.e., there are no ties), then they form a $T$-locally optimal codeword for some $T < \infty$. Moreover, $\hat{x}$ is the LP optimal and, hence, ML codeword.

**Proof:** From Theorem 11, we know that $\hat{x}$ is a codeword. To prove that $\hat{x}$ is a $T$-locally optimal codeword, we have to show that for the projection $\pi(u^{(\omega)})$ of any generalized minimal $T$-local deviation $u^{(\omega)}$, the inequality

$$\langle \hat{x} \oplus c \pi(u^{(\omega)}), \gamma \rangle > \langle \hat{x}, \gamma \rangle$$

holds, where $c > 0$ is a scaling factor such that $c \pi_i(u^{(\omega)}) \leq 1$ for all $i \in 1, 2, \ldots, n$, and $(\hat{x} \oplus c \pi(u^{(\omega)}))_i = |\hat{x}_i - c \pi_i(u^{(\omega)})|$ is as defined in [16]. Without loss of generality, we assume that $u^{(\omega)}$ is rooted at $i_0$ and consider the correlation of $\hat{x} \oplus \pi(u^{(\omega)})$ and $\gamma$. This gives

$$\langle \hat{x} \oplus c \pi(u^{(\omega)}), \gamma \rangle = \sum_{i=1}^{n} \left| \hat{x}_i - c \pi_i(u^{(\omega)}) \right| \gamma_i$$

$$= \langle \hat{x}, \gamma \rangle + c \sum_{i=1}^{n} \sum_{t=0}^{T} \beta^t \sum_{m \in N(i_0, 2^t): m \sim i} (-1)^{\hat{x}_m} u_m \gamma_i$$

$$= \langle \hat{x}, \gamma \rangle + c U^T_{i_0}(\hat{x}, u),$$

where $U^T_{i_0}(\hat{x}, u)$ is as defined in (48).

To show that $U^T_{i_0}(\hat{x}, u) > 0$, consider a tree $T^I_{i_0}$ with large $I$. Since the WMS algorithm converges to a WMS-consistent message vector, the assignment for the subtree $T^I_{i_0}$ is the same as $\hat{x}$ for some $T < \infty$. Here, Lemma 36 is required because the leaf assignment may not match a codeword. Also, $u$
can be obtained from the generalized minimal valid deviation $\tilde{u}$ on $T_{i_0}^{2I}$ by truncating

$$u_m = \begin{cases} \tilde{u}_m & \text{if } m \in N(i_0, 2t) \text{ for some } 0 \leq t \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma [36], we can conclude that $U_T^T(\hat{x}, u) > 0$. Therefore, $\hat{x}$ is a $T$-locally optimal codeword.

According to [16, Theorem 4] or [17, Theorem 6], and by Lemma [38] the $T$-local optimality of $\hat{x}$ implies that $\hat{x}$ is the unique optimal LP solution given the LLR $\gamma$. Since $\hat{x} \in \{0, 1\}^n$ is an integer codeword, $\hat{x}$ is also an ML codeword.

**Appendix G**

**Another proof of Lemma [38]**

In this appendix, we extend the result of [16, Lemma 4] to the case when tree depth is greater than $\frac{1}{2}\text{girth}(G)$. For a given non-zero LP solution $z \in [0, 1]^n$, we first introduce the construction of the computation trees $T_{i}^{2I}(z)$ for all $i \in V_L$ with $z_i > 0$. Then, the distribution over skinny subtrees of $T_{i}^{2I}(z)$ is introduced. With the defined distribution, the symmetry property of the probabilities of a directed path and the corresponding reverse path in $G$ is discussed. Finally, we show that $z$ can represented by a linear scaling of the expected value of bit nodes.

For each $i \in V_L$ and $z_i \neq 0$, consider the depth-$2I$ computation tree $T_{i}^{2I} = (I \cup J, E')$. Let $\hat{i}$ and $\hat{j}$ be the variable nodes and check nodes in $T_{i}^{2I}$, respectively. We first remove the variable nodes $\{\hat{i} \in I : z_{\eta(\hat{i})} = 0\}$ and the edges incident to these variable nodes from $T_{i}^{2I}$. After the first removal, any nodes that are unreachable from $i$ are removed as well. The remainder of the tree is denoted by $T_{i}^{2I}(z)$. Note that the distance from $i$ to every leaf of $T_{i}^{2I}(z)$ is also $2I$.

To construct a probability distribution over all skinny subtrees in $T_{i_0}^{2I}(z)$, we first define the transition probability between two distinct neighbors of a check node. For any check node $j \in V_R$, the definition of the LP polytope implies that $z$ can be rewritten as

$$z = \sum_{w \in R_j} \alpha_w w,$$

where $R_j = \{w \in \{0, 1\}^n : \sum_{i \in N(j)} w_i \equiv 0 \mod 2\}$, $\alpha_w \geq 0$ and $\sum_{w \in R_j} \alpha_w = 1$. The coefficient $\alpha_w$ can be regarded as a probability distribution over $R_j$, and

$$z_i = \sum_{w \in R_j} \alpha_w w_i.$$
is the expected value of the \( i \)th variable node of \( \mathcal{G} \). For a \( j \in \mathcal{V}_R \) and an \( i \in \mathcal{N}(j) \) with \( w_i = 1 \), given that “\( j \) is reached from \( i \)”, we define the probability of moving to \( m \in \mathcal{N}(j) \setminus i \) (i.e. the transition probability from \( i \) to \( m \)) by

\[
p(m|i, j) \triangleq \frac{1}{z_i} \rho_j(i, m),
\]

where \( \rho_j(i, m) \triangleq \sum_{w \in \mathcal{R}_j, w_i = 1} \left( \sum_{m' \in \mathcal{N}(j) \setminus i} w_{m'} \right)^{-1} \alpha_w w_m \). Note that

\[
\sum_{m \in \mathcal{N}(j) \setminus i} \rho_j(i, m) = \sum_{m \in \mathcal{N}(j) \setminus i} \frac{\sum_{m' \in \mathcal{N}(j) \setminus i} \alpha_w w_m}{\left( \sum_{m' \in \mathcal{N}(j) \setminus i} w_{m'} \right)} = z_i,
\]

and, if \( w_m = 1 \),

\[
\rho_j(m, i) = \sum_{w \in \mathcal{R}_j \atop w_m = 1} \frac{\alpha_w w_i}{\sum_{m' \in \mathcal{N}(j) \setminus i} w_{m'}} = \sum_{w \in \mathcal{R}_j \atop w_m = 1} \frac{\alpha_w w_m}{\sum_{m' \in \mathcal{N}(j) \setminus i} w_{m'}} = \rho_j(i, m).
\]

After having the transition probability, we then define a probability distribution over skinny subtrees of \( \mathcal{T}_{2I}^i(z) \). Let \( \mathcal{A}_i(z, 2I) \) be the set of all connected skinny subtrees of \( \mathcal{T}_{2I}^i(z) \). For a fixed \( \tau \in \mathcal{A}_i(z, 2I) \), let \( \mathcal{I}_{\ell, \tau} \) and \( \mathcal{J}_{\ell, \tau} \) be the set of variable nodes and the set of check nodes in the \( \ell \)th level of \( \tau \), respectively. For each \( \ell \in \{1, \ldots, I\} \), define \( \mathcal{B}_\ell(\tau) \triangleq \{ (\hat{i}, \hat{j}, \hat{m}) \in \mathcal{I}_{\ell, 2(\ell - 1)} \times \mathcal{J}_{\ell, 2\ell - 1} \times \mathcal{I}_{\ell, 2\ell} : (\hat{i}, \hat{j}, \hat{m}) \in \tau \} \) as the set of all paths from the \( 2(\ell - 1) \)th level of \( \tau \) to the \( 2\ell \)th level of \( \tau \). The probability distribution over the skinny trees \( \tau \in \mathcal{T}_{2I}^i(z) \) is defined by

\[
p_{i0}(\tau) \triangleq \prod_{\ell=1}^{I} \prod_{(\hat{i}, \hat{j}, \hat{m}) \in \mathcal{B}_\ell(\tau)} p(\eta(\hat{m})|\eta(\hat{i}), \theta(\hat{j})) = \prod_{\ell=1}^{I} \prod_{(\hat{i}, \hat{j}, \hat{m}) \in \mathcal{B}_\ell(\tau)} \frac{1}{z_{i(\hat{i})}} \rho_{\theta(j)}(\eta(\hat{i}), \eta(\hat{m})).
\]

(50)

Let \( \mathcal{B}_\ell(\tau) \triangleq \mathcal{A}_i(z, \mathcal{T}_{2I}^2 \setminus \tau) \) be a variable node at \( 2\ell \)th level of \( \mathcal{T}_{2I}^i(z) \). When a skinny subtree, \( \tau \), of \( \mathcal{T}_{2I}^i(z) \) is randomly selected according to the distribution \( \rho_{\mathcal{B}_\ell}(\tau) \), the probability of having \( \mathcal{B}_\ell \) in \( \tau \) is

\[
p_{i0}(\mathcal{B}_\ell \setminus \mathcal{B}_\ell') = \sum_{\tau' \in \mathcal{A}_i(z, 2I)} p_{i0}(\tau') \mathbb{1}(\mathcal{B}_\ell \setminus \mathcal{B}_\ell'),
\]

(51)

where \( \mathbb{1}(\cdot) \) is an indicator function, which is 1 if \( \mathcal{B}_\ell \) is in \( \tau \), and is 0 otherwise. It is clear that there is a unique path in \( \mathcal{T}_{2I}^i(z) \) from \( i_0 \) to \( \mathcal{B}_\ell \). Let the path be \( b \triangleq (b_0, b_1, \ldots, b_{2\ell}) \), where \( b_0 = i_0 \), \( b_{2\ell} \in \mathcal{I} \) for \( \ell = 0, 1, \ldots, T \) and \( b_{2\ell+1} \in \mathcal{J} \) for \( \ell = 0, 1, \ldots, T - 1 \). By substituting (50) into (51), we have

\[
p_{i0}(\mathcal{B}_\ell) = \prod_{\ell=0}^{T-1} \frac{1}{z_{i(b_{2\ell})}} \rho_{\theta(b_{2\ell+1})}(\eta(b_{2\ell}), \eta(b_{2\ell+2})).
\]
Let \( j_{2\ell+1} = \theta(b_{2\ell+1}) \) for \( \ell = 0, 1, \ldots, T - 1 \), and \( i_{2\ell} = \eta(b_{2\ell}) \) for \( \ell = 1, 2, \ldots, T \). The RHS of (52) becomes

\[
p_{i_{2\ell}}(b_{2T}) = \prod_{\ell=0}^{T-1} \frac{1}{z_{i_{2\ell}}^{\eta(c_{2\ell})}} \rho_{j_{2\ell+1}}(i_{2\ell}, i_{2\ell+2}).
\]  

(53)

Since \((i_0, j_1, i_2, \ldots, j_{2T-1}, i_{2T})\) also forms a directed path from \(i_0\) to \(i_{2T}\) in \(G\), and \(z_{i_{2\ell}} = z_{\eta(b_{2\ell})} > 0\) for all \(\ell = 0, 1, \ldots, T\), there is a path \(c = (c_0, c_1, \ldots, c_{2T})\) in \(T_{i_{2\ell}}^{2T}\) with \(c_0 = i_{2T}\), \(c_{2\ell} \sim i_{2T-2\ell}\) for \(\ell = 1, \ldots, T\) and \(c_{2\ell+1} \sim j_{2T-2\ell-1}\) for \(\ell = 0, 1, \ldots, T - 1\). Note that the path \(c\) is associated with the reverse path of \((i_0, j_1, i_2, \ldots, j_{2T-1}, i_{2T})\). Similarly, by drawing a skinny subtree from \(A_{i_{2\ell}}(z, 2I)\), the probability of having \(c_{2T}\) in the skinny tree is

\[
p_{i_{2\ell}}(c_{2T}) = \prod_{\ell=0}^{T-1} \frac{1}{z_{i_{2\ell}}^{\eta(c_{2\ell})}} \eta(c_{2\ell+1}) \eta(c_{2\ell+2})\]

\[
= \prod_{\ell=0}^{T-1} \frac{1}{z_{i_{2\ell+1}}^{\eta(c_{2\ell})}} \rho_{j_{2\ell+1}}(i_{2\ell+1}, i_{2\ell+2}).
\]  

(54)

From (54), the probabilities \(p_{i_{2\ell}}(b_{2T})\) and \(p_{i_{2\ell}}(c_{2T})\) satisfy the symmetry property

\[
z_{i_{2\ell}}p_{i_{2\ell}}(c_{2T}) = \prod_{\ell=0}^{T-1} \frac{1}{z_{i_{2\ell}}} \rho_{j_{2\ell+1}}(i_{2\ell+1}, i_{2\ell+2}) \]

\[
= \prod_{\ell=0}^{T-1} \frac{1}{z_{i_{2\ell}}} \rho_{j_{2\ell+1}}(i_{2\ell+1}, i_{2\ell+2})\]

\[
= z_{i_0}p_{i_0}(b_{2T}),
\]  

(55)

where the equality (a) is from (49), and the equality (b) is from (53).

For a variable node \(m \in V_L\) and a \(T \leq I\), let \(\mathcal{M}_m(\tau, 2T)\) be the subset of variable nodes associated with \(m\) and in the \(2T\)th level of a skinny tree \(\tau\). The expected value of the size of \(\mathcal{M}_m(\tau, 2T)\) given \(\tau \in T_{i_0}^{2T}(z)\), denoted by \(M_{m,i_0}(2T)\), is

\[
M_{m,i_0}(2T) = \sum_{\tau \in A_{i_0}(z, 2I)} p_{i_0}(\tau) |\mathcal{M}_m(\tau, 2T)|.
\]

\[
= \sum_{\hat{m} \in M_m(T_{i_0}^{2T}(z), 2T)} \left( \sum_{\tau \in A_{i_0}(z, 2I)} p_{i_0}(\tau) \mathbb{1}(\hat{m} \in \tau) \right)
\]

\[
= \sum_{\hat{m} \in M_m(T_{i_0}^{2T}(z), 2T)} p_{i_0}(\hat{m}),
\]  

(56)

where \(M_m(T_{i_0}^{2T}(z), 2T)\) is the set of variable nodes associated with \(m\) and in the \(2T\)th level of \(T_{i_0}^{2T}(z)\), the equality (a) is from the fact that any \(\hat{m} \in M_m(\tau, 2T)\) is also in the \(2T\)th level of \(T_{i_0}^{2T}(z)\), and the
equality (b) is from \(51\). In \(T_{i_0}^{2I}(z)\), the path from \(i_0\) to each \(\hat{m}\) \(\in M_m(T_{i_0}^{2I}(z), 2T)\) is associated with a unique length-\(2T\) path from \(i_0\) to \(m\) in \(G\), and the corresponding length-\(2T\) reverse path from \(m\) to \(i_0\) in \(G\) is also associated with a unique path from \(m\) to a variable node \(\hat{i} \in M_{i_0}(T_{i_0}^{2I}(z), 2T)\) in \(T_{i_0}^{2I}(z)\). By \(55\) and \(56\), we can have another symmetry property

\[
\begin{align*}
  z_{i_0} \sum_{\tau \in A_{i_0}(z,2I)} p_{i_0}(\tau) |M_m(\tau,2T)| &= \sum_{\hat{m} \in M_m(T_{i_0}^{2I}(z),2T)} z_{i_0}p_{i_0}(\hat{m}) \\
  &= \sum_{\hat{i} \in M_{i_0}(T_{i_0}^{2I}(z),2T)} \sum_{\tau \in A_m(\tau,2I)} z_m p_m(\hat{i}) \\
  &= z_m \sum_{\tau \in A_m(\tau,2I)} p_m(\tau) |M_{i_0}(\tau,2T)|. 
\end{align*}
\]

(57)

With the above observations, we can start to prove Lemma \(38\).

**Proof:** Let the probability of choosing \(i \in V_L\) as the root of a skinny tree be \(p(i) = z_i/\|z\|_1\). Then, for any \(i \in V_L\) with \(z_i > 0\), and any \(I > 0\) we can write

\[
E[X_i] = \frac{1}{\|z\|_1} \sum_{\ell=0}^{I} \sum_{v \in V_L} \frac{1}{\|z\|_1} \left( \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) |M_v(\tau,2\ell)| \right) \\
= \frac{1}{\|z\|_1} \sum_{\ell=0}^{I} \sum_{v \in V_L} \frac{1}{\|z\|_1} \left( \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) |M_v(\tau,2\ell)| \right). 
\]

(58)

By \(57\), the last term in the RHS of \(58\) is equal to \(z_i \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) |M_v(\tau,2\ell)|\). Thus,

\[
E[X_i] = \frac{1}{\|z\|_1} \sum_{\ell=0}^{I} \sum_{v \in V_L} \frac{z_i}{\|z\|_1} \left( \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) |M_v(\tau,2\ell)| \right) \\
= \frac{1}{\|z\|_1} \sum_{\ell=0}^{I} \frac{z_i}{\|z\|_1} \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) \sum_{v \in V_L} |M_v(\tau,2\ell)|. 
\]

When \(G\) is a \((d_v,d_c)\)-regular bipartite graph, the number of variable nodes at the \(\ell\)th level of \(\tau\) is

\[
\sum_{v \in V_L} |M_v(\tau,2\ell)| = d_v(d_v-1)^{\ell-1}. 
\]

Thus, we have

\[
E[X_i] = \frac{1}{\|z\|_1} \sum_{\ell=0}^{I} \frac{z_i}{\|z\|_1} \sum_{\tau \in A_v(z,2I)} p_{\tau}(\tau) \left( d_v(d_v-1)^{\ell-1} \right) \\
= \frac{z_i}{\|z\|_1} \left( 1 + \sum_{\ell=1}^{I} \frac{d_v d_v}{\ell} (d_v-1)^{\ell-1} \right),
\]

and this concludes the proof of Lemma \(38\).

\(\blacksquare\)
REFERENCES

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo-codes,” in *Proc. IEEE Int. Conf. Commun.*, vol. 2. Geneva, Switzerland: IEEE, May 1993, pp. 1064–1070.

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

[3] D. J. C. MacKay, “Good error-correcting codes based on very sparse matrices,” *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[4] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, “Design of capacity-approaching irregular low-density parity-check codes,” *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[5] N. Wiberg, “Codes and decoding on general graphs,” Ph.D. dissertation, Linköping University, S-581 83 Linköping, Sweden, 1996.

[6] N. Wiberg, H.-A. Loeliger, and R. Kötter, “Codes and iterative decoding on general graphs,” *Eur. Trans. Telecom.*, vol. 6, no. 5, pp. 513–525, Sept. – Oct. 1995.

[7] B. J. Frey and R. Koetter, “Exact inference using the attenuated max-product algorithm,” in *Advanced Mean Field Methods: Theory and Practice*, M. Opper and D. Saad, Eds. Cambridge, MA: MIT Press, 2000.

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

[9] Y. Weiss and W. T. Freeman, “On the optimality of solutions of the max-product belief-propagation algorithm in arbitrary graphs,” *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 763–784, Feb. 2001.

[10] M. J. Wainwright, T. S. Jaakkola, and A. S. Willsky, “MAP estimation via agreement on trees: Message-passing and linear programming,” *IEEE Trans. Inform. Theory*, vol. 51, no. 11, pp. 3697–3717, Nov. 2005.

[11] J. Feldman, M. J. Wainwright, and D. R. Karger, “Using linear programming to decode binary linear codes,” *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 954–972, March 2005.

[12] R. Koetter and P. O. Vontbel, “Graph covers and iterative decoding of finite-length codes,” in *International Symposium on Turbo Codes and Related Topics*, Brest, France, Sept. 2003, pp. 75–82.

[13] J. Feldman, T. Malkin, R. A. Servedio, C. Stein, and M. J. Wainwright, “LP decoding corrects a constant fraction of errors,” *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 82–89, Jan. 2007.

[14] C. Daskalakis, A. G. Dimakis, R. M. Karp, and M. J. Wainwright, “Probabilistic analysis of linear programming decoding,” *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3565–3578, 2008.

[15] R. Koetter and P. O. Vontbel, “On the block error probability of LP decoding of LDPC codes,” in *Proc. 1st Annual Workshop on Inform. Theory and its Appl.*, San Diego, CA, Feb. 2006.

[16] S. Arora, C. Daskalakis, and D. Steurer, “Message-passing algorithms and improved LP decoding,” in *Proceedings of the 41st annual ACM symposium on Symposium on theory of computing*, Bethesda, MD, USA, 2009, pp. 3–12.

[17] N. Halabi and G. Even, “LP decoding of regular ldpc codes in memoryless channels,” Feb. 2010, [Online]. Available: http://arxiv.org/abs/1002.3117.

[18] J. Chen and M. P. C. Fossorier, “Density evolution for two improved BP-based decoding algorithms of LDPC codes,” *IEEE Commun. Letters*, vol. 6, no. 5, pp. 208–210, 2002.

[19] Y.-Y. Jian and H. D. Pfister, “Convergence of weighted min-sum decoding via dynamic programming on coupled trees,” in *Proc. Int. Symp. on Turbo Codes & Iterative Inform. Proc.*, Brest, France, Sept. 2010.

[20] V. Kolmogorov and M. J. Wainwright, “On the optimality of tree-reweighted max-product message-passing,” in *Uncertainty in Artificial Intelligence*, Edinburgh, Scotland, UK, 2005.
[21] P. O. Vontobel, “A factor-graph-based random walk, and its relevance for LP decoding analysis and Bethe entropy characterization,” in Proc. Annual Workshop on Inform. Theory and its Appl., San Diego, CA, Feb. 2010.