Joint Demodulation and EMS Decoding Algorithm for \(Q\)-ary LDPC Codes

Wei Lin, Baoming Bai, Sheng Tong

State Key Lab. of Integrated Services Networks, Xidian University, Xi’an 710071, China
linwei@mail.xidian.edu.cn

Abstract

To reduce the high decoding complexity of \(q\)-ary LDPC codes, a joint-demodulation and extended min-sum (JD-EMS) decoding algorithm is presented in this paper. By utilizing the squares of the distances between signal and constellation points over constellation graph as the decoder input soft messages, the proposed algorithm not only facilitates the computations of the decoder initial messages, but also avoids the performance loss due to conversions between probabilities and log-likelihood-ratios. The elementary check node (ECN) processing is also improved in JD-EMS algorithm, thus the number of real additions can be reduced. Moreover, we also give an upper bound of the number of comparison candidates in the sorter at each ECN step. Simulation results indicate that, while significantly reducing the number of real additions at check nodes, JD-EMS algorithm performs as well as EMS algorithm on both AWGN and Rayleigh fading channels.

Keywords: LDPC Codes, Extended Min-Sum, Bubble-Check

1. Introduction

Since Davey et al. generalized binary low-density parity-check codes to finite fields \(\text{GF}(q)\) with \(q>2\) in 1998 [1], extensive studies indicate that, \(q\)-ary LDPC (QLDPC) codes outperform their binary counterparts and other coding schemes at short or medium lengths [2]-[6]. Furthermore, QLDPC codes have stronger capability to overcome burst errors [8], and are more appropriate to be combined with high order modulation schemes. However, using \(q\)-ary sum-product algorithm (QSPA) [1], the decoding complexity of QLDPC codes is dominated by \(O(q^n)\). Therefore, high decoding complexity inhibits the practical applications of QLDPC codes.

To reduce the decoding complexity of QLDPC codes, various complexity-reduced decoding algorithms have been proposed. Barnault et al. implemented fast Fourier transforms (FFT) to check node steps of QSPA, and reduced the decoding complexity to \(O(q \log q)\) [7]. However, large amount of real multiplications and the issues of quantizing messages in probability domain prevent the applications of the algorithm. Meanwhile, Song et al. preserved FFT operations in check node steps while representing the decoding messages in the combined domain of probabilities and log likelihood ratios (LLR) [8], but the mass look up table (LUT) operations make the complexity of the algorithm still too high. To avoid the real multiplication operations, Wymeersch et al. proposed the so-called Log-SPA algorithm in LLR domain [9], but the decoding computational complexity is still in the order of \(O(q^n)\), thus the algorithm is not appropriate for practical applications when \(q>16\).

In 2007, Declercq et al. proposed the so-called extended min-sum (EMS) algorithm [10], which was soon improved by Voicila et al. in [11]. By truncating the length of messages to \(n_c \ll q\), EMS algorithm reduces the computational complexity of real additions to \(O(n_c \log n_c)\). However, for hardware implementations, the complexity of real comparisons is no less than that of real additions, thus the complexity of EMS algorithm is actually dominated by \(O(n_c^2)\). To reduce the computational complexity of real comparisons, Boutillon et al. proposed the bubble-check algorithm for elementary check node (ECN) processing of EMS algorithm, and efficiently reduces the decoding computational complexity to \(O(n_c \sqrt{n_c})\) [12].

In this paper, we propose a joint demodulation and extended min-sum (JD-EMS) decoding algorithm for QLDPC codes. Combining the demodulator and decoder, the JD-EMS algorithm utilizes the squares of the distances between signal and constellation points over constellation graph as the
Joint Demodulation and EMS Decoding Algorithm for $Q$-ary LDPC Codes
Wei Lin, Baoming Bai, Sheng Tong
Journal of Convergence Information Technology, Volume 6, Number 6, June 2011

decoder input soft messages. According to the distribution of messages at ECN processing, the bubble-check algorithm is also improved in this paper, and the number of real additions at ECN processing can be effectively reduced. Moreover, we also give an upper bound of the number of comparison candidates in the sorter at each ECN step, thus the length of the sorter $n_s$ can be selected more accurate. Simulation results indicate that, JD-EMS algorithm performs as well as EMS algorithm on both AWGN and Rayleigh fading channels while efficiently reducing the number of real additions at ECN processing, thus is appropriate for practical communication systems.

2. $Q$-ary LDPC codes

To facilitate the description, we denote the elements over $\text{GF}(q)$ as $\{0,1,\ldots,q-1\}$, and the latter $q-1$ elements constitute the set of nonzero elements $\text{GF}(q) \setminus \{0\}$. Let $H = \{h_{ij}\}_{M \times N}$ present the parity-check matrix of a QLDPC code, then the element $h_{ij} \in \text{GF}(q)$. For $H$ should be a sparse matrix, thus the majority of elements in $H$ are ‘0’s. Let $v=(v_0,v_1,\ldots,v_{N-1})$ be a codeword of the QLDPC code, then $vH^T = 0$, i.e.,

$$
\sum_{j:\ h_{ij} \in \text{GF}(q) \setminus \{0\}} h_{ij} \otimes v_j = 0, \quad \text{for} \ i = 0,1,\ldots,M-1
$$

(1)

where additions $\otimes$ and multiplications $\otimes$ are the operations defined over $\text{GF}(q)$.

Figure 1 illustrates the Forney style factor graph of a regular QLDPC code with parameter $(d_v,d_c)$, where $d_v$ denotes the degree of variable nodes, and $d_c$ denotes the degree of check nodes. Variable node $V_j$, $j=0,\ldots,N-1$, corresponds to the $j$-th column of $H$, check node $C_i$, $i=0,\ldots,M-1$, corresponds to the $i$-th row of $H$. Therefore, the QLDPC code can be iteratively decoded by passing and updating messages among nodes on the factor graph. Different from binary LDPC codes, the messages of QLDPC codes are vectors of length $q$, and each element represents the likelihood value of the associated $\text{GF}(q)$ symbol. In addition, the permutation nodes multiply the associated $\text{GF}(q)$ symbols of the message vectors with nonzero elements over $\text{GF}(q)$, thus the passing-by message vectors are permuted.

3. EMS algorithm

Representing the decoding messages of QLDPC codes in LLR domain, the message vectors of length $q$ should be in the form of
Joint Demodulation and EMS Decoding Algorithm for $Q$-ary LDPC Codes
Wei Lin, Baoming Bai, Sheng Tong
Journal of Convergence Information Technology, Volume6, Number 6, June 2011

$$L_{\beta} = [L[0], L[1], \ldots, L[q-1]],$$

Where

$$L[\beta] = \log \frac{P(\beta)}{P(0)} \quad \text{for} \quad \beta \in \{0, 1, \ldots, q-1\}$$

denotes the LLR measure of variable $V$ taking value on $\beta$, and $P(\beta)$ denotes the corresponding probability measure. Arrange $L_{\beta}$ in decreasing order, and then truncate the preceding $n_u$ terms, the message vector of EMS algorithm is obtained, i.e., $U = [U[0], U[1], \ldots, U[n_u-1]]$. Let $U^{gr}[i]$ denote the associated GF($q$) symbol of $U[i]$, then vector $U^{gr} = [U^{gr}[0], U^{gr}[1], \ldots, U^{gr}[n_u-1]]$ is the GF($q$) index vector of $U$. For the symbols beyond $U^{gr}$, we denote their associated LLR values as $\gamma_{v} = U[n_u] - \delta$, where $\delta$ is an optimized value.

3.1. Standard EMS algorithm

Let $U_{VC}$ denote the message vector transmitted from variable node $V$ to check node $C$, and let $U_{CV}$ denote the message vector transmitted from check node $C$ to variable node $V$. Utilizing the well-known forward/backward strategy [9], a node updating step can be decomposed into several elementary steps. In algorithm description, we only give the elementary variable node (EVN) processing and the ECN processing for simplicity. Denote the input message vectors of EVN and ECN processing as $V$ and $I$, and the corresponding output message vector as $U$. Let $L_{v}$ be the channel initial message, then the standard EMS algorithm can be briefly described as follows:
1) Initialization: initialize $U_{VC}$ to the maximum $n_u$ terms of $L_{v}$;
2) Permutation: permute $U_{VC}^{gr}$ according to the corresponding permutation node;
3) ECN processing: define a set $\{M[k], 0 \leq k < n_u\}$ such that

$$M[k] = \max_{i,j \in \{0,n_u-1\}} \{V[i] + I[j], \max_{i,j \in \{0,n_u-1\}} V[i] + I[j] \},$$

and $M^{gr}[k]$ denotes the GF($q$) index symbol of $M[k]$. Then output $U$ is obtained by arranging the $n_u$ largest values of $M$ in decreasing order.
4) Inverse permutation: inverse permute $U_{VC}^{gr}$ according to the corresponding permutation node;
5) EVN processing: define a length $2n_u$ vector $Z = [Z[0], \ldots, Z[2n_u-1]]$ with

$$Z[i] = V[i] + X, \quad Z[n_u + i] = I[i] + \gamma_{v}, \quad \text{for} \quad i \in \{0, n_u - 1\}$$

where

$$X = \begin{cases} I[j], & I^{gr}[j] = V^{gr}[i] \\ \gamma_{v}, & I^{gr}[j] \neq V^{gr}[i] \end{cases}, \quad \text{for} \quad j \in \{0, n_u - 1\}.$$ 

The output $U$ is obtained by arranging the $n_u$ largest values of $Z$ in decreasing order.
6) Decision: temporarily decide variable $V$ to the first term of $U^{gr}$, if the parity-check equations are fulfilled or the maximum iteration is arrived, halt decoding, else return to step 2);
Joint Demodulation and EMS Decoding Algorithm for $Q$-ary LDPC Codes
Wei Lin, Baoming Bai, Sheng Tong
Journal of Convergence Information Technology, Volume 6, Number 6, June 2011

Figure 2. An example of the 4-th step of standard ECN processing

The computational complexity of EMS algorithm mostly relies on the ECN processing, and a standard ECN processing algorithm is given in [11]. To facilitate the computation, an $n_v \times n_u$ matrix $M$ with component $M[i, j] = V[i] + I[j]$ is introduced, and let $M^{G^R}[i, j]$ be the GF($q$) index of $M[i, j]$, i.e., $M^{G^R}[i, j] = V^{G^R}[i] \oplus I^{G^R}[j]$. Initializing the first column of $M$ into the length-$n_v$ sorter $S$, the ECN steps can be described as follows:

For $k = 1$ to $K_{\text{max}}$ loop:
   a) Extract the largest value in $S$, i.e., $M[i, j]$. If $M^{G^R}[i, j]$ has never been introduced into $U^{G^R}$, move $M[i, j]$ into $S$;
   b) Compute $M[i, j + 1] = V[i] + I[j + 1]$ and replace the extracted value in $S$ by $M[i, j + 1]$;

There might be repeating symbols during the loops, the maximum number of loops $K_{\text{max}}$ is often around $n_v + 2$. Figure 2 illustrates an example of the 4-th step of standard ECN processing, where the black circles (GC) represent the values that have been introduced into $S$, and the dashed circle (DC) represents the temporarily maximum value in $S$. After excluding the DC from $S$, the next value to be moved in $S$ should be $M[2, 1]$.

3.2. Bubble-Check ECN processing

There are large amount of real comparisons in standard ECN processing, thus the complexity is still very high. To reduce the number of real comparisons, the bubble-check (BC) ECN processing reduces the length of the sort $S$ from $n_v$ to $n_b = \sqrt{2n_v}$ by introducing a flag variable $T$ [12]. Initializing the preceding $n_b$ values in the first column of $M$ into the length-$n_b$ sorter $S$, the BC ECN steps can be described as follows:

For $k = 1$ to $K_{\text{max}}$ loop:
   a) Extract the largest value in $S$, i.e., $M[i, j]$. If $M^{G^R}[i, j]$ has never been introduced into $U^{G^R}$, move $M[i, j]$ into $S$;
   b) Flag control: if $i = 0$, then set $(T = 1, T = 0)$; if $j = 0$ and $i \geq n_b - 1$, then set $(T = 0, T = 1)$;
   c) If $M[i + T, j + T]$ has never been moved into $S$, then compute $M[i + T, j + T] = V[i + T] + I[j + T]$ and introduce it in $S$, else compute $M[i + T, j + T] = V[i + T] + I[j + T]$ and introduce it in $S$;

Figure 3. An example of the 5-th step of BC ECN processing

An example of the 5-th step of BC ECN processing is illustrated in Figure 3, where $n_b = 4$. It can be seen that, the temporarily maximum value in $S$ is $M[3, 0]$, and the value to substitute $M[3, 0]$ in $S$ should be $M[4, 0]$. 

- 479 -
To analyze the number of comparison candidates in $S$ at each ECN step, we rewrite the Property 1 in [12] as follows.

Property 1: For $(i, j, i', j') \in [0, n_q - 1]^4$, if $i \leq i'$ and $j \leq j'$, then $M[i, j] \leq M[i', j']$.

By exploiting Property 1, we can see that not all values in $S$ have to be compared at each ECN step. For example, at the first ECN step, the maximum value in $S$ is definitely $M[0, 0]$. At the second ECN step, the maximum value in $S$ should be $M[0, 1]$ or $M[1, 0]$. Therefore, at the $k$-th ECN step, the values that necessarily have to be compared in $S$ are defined as bubbles, and the maximum number of bubbles is denoted by $n_{\text{max}}(k)$. Let $\tau_s = 1 + s(s + 1)/2$, then the bubbles should be in an upper triangular shape in the worst case, and $n_{\text{max}}(\tau_s) = s + 1$. Referring to Property 1 again, it can be seen that in case $k \in [\tau_{s-1}, \tau_s)$, the maximum number of bubbles should be $n_{\text{max}}(\tau_s) = s$. Then, we obtain

$$n_{\text{max}}(k) = s + 1, \quad \frac{s^2 + s + 2}{2} \leq k < \frac{s^2 + 3s + 4}{2},$$

where $s = 0, 1, \ldots$. Solving (7), the explicit upper bound of the number of bubbles at the $k$-th ECN processing should be

$$n_{\text{max}}(k) = \left\lfloor \frac{1 + \sqrt{1 + 8(k - 1)}}{2} \right\rfloor, \quad \text{for} \quad k = 1, 2, \ldots, \quad (8)$$

where $\lfloor x \rfloor$ denotes the integer part of $x$. According to (8), the length $n_k$ of the sorter $S$ can be set more accurate.

4. JD-EMS algorithm

In this section, the proposed JD-EMS algorithm is given in detail. First, we develop the method for computing the initial messages of the decoder. Then, after analyzing the distribution of the messages at ECN steps, we give the explicit ECN processing of JD-EMS algorithm.

4.1. Computation of initial messages

Consider a QLDPC code being combined with an order-$q$ modulation scheme, i.e., $q$-QAM, then the cardinality of the signal constellation equals that of the finite field, and the correspondence between constellation symbols and code symbols is one-to-one. Let $A_p = x_p + j y_p$ represents the constellation symbol which corresponds to the code symbol $\beta \in GF(q)$, and denote the position of the received signal on the constellation graph as $A_s = x_s + j y_s$. Furthermore, we define the Euclidean distance $d_p$ between $A_s$ and $A_p$ as follows:

$$d_p = |A_p - A_s|^2 = (x_p - x_s)^2 + (y_p - y_s)^2.$$  \hspace{1cm} (9)

Then on AWGN channels, the probability of the received signal taking value on $A_p$ should be

$$P(\beta) = \frac{\exp \left[ -\frac{d_p^2}{2\sigma^2} \right]}{\sum_{\beta \in GF(q)} \exp \left[ -\frac{d_{\beta}^2}{2\sigma^2} \right]}.$$  \hspace{1cm} (10)

where $2\sigma^2$ denotes the power of channel noises. For EMS algorithm, the LLR value of symbol $\beta$ can be computed by equation (3). Substitute the probabilities in (3) by (10), then
Joint Demodulation and EMS Decoding Algorithm for $Q$-ary LDPC Codes
Wei Lin, Baoming Bai, Sheng Tong
Journal of Convergence Information Technology, Volume 6, Number 6, June 2011

\[ L(\beta) = \log \frac{P(\beta)}{P(0)} = \frac{1}{2\sigma^2}(d^2_h - d^2_p). \]  

(11)

Since $2\sigma^2$ and $d^2_p$ are constants for one code symbol, we can consider utilizing $d^2_p$ directly as the initial message of the decoder. The situation on Rayleigh fading channel is similar to that on AWGN channel, and the initial message of the decoder can be considered to be $D_0 = |A_s - A_d|$, where $A_s = x_s + jy_s$ denotes the channel fading coefficient. Apparently, $d^2_p$ and $D^2_0$ are inversely proportional to the probability of the received signal taking value on $A_s$.

Take AWGN channel for example, assume $d^2_p$ be the minimum value in the set $\mathbb{D} = \{d^2_i, i \in [0, q-1]\}$.

Take the $n_s$ minimum values in $\mathbb{D}$ and arrange them in increasing order, vector $\mathbf{D} = \{D[0], ..., D(n_s - 1)\}$ is obtained, and $D[0] = d^2_p$. Then minus each term in $\mathbf{D}$ by $D[0]$, and the initial message vector of the JD-EMS decoder $\mathbf{U} = \{U[0], ..., U[n_s - 1]\}$ is obtained. Apparently, $U[0] = d^2_s - d^2_p = 0$, which is the key issue to reduce the number of real additions in ECN processing.

4.2. Message distribution and ECN processing

For ECN processing of JD-EMS algorithm, the first terms of the two inputs $\mathbf{V}$ and $\mathbf{I}$ are ‘0’s. Thus the first column $[M[0,0], M[1,0], ..., M(n_s-1,0)]^T$ in the matrix $\mathbf{M}$ should actually be $\mathbf{V}^T$, and $M[i,0] = V[i] + I[0] = V[i]$. Similarly, the first row of $\mathbf{M}$ should be $\mathbf{I}$, and $M[0,j] = V[0] + I[j] = I[j]$.

![Figure 4. Distribution of the elements of E in M](image)

Let $\mathbf{E}$ denote the set of the first column and the first row of $\mathbf{M}$, then in case the values to be moved into the sorter $\mathbf{S}$ belongs to $\mathbf{E}$, real additions can be avoided. Figure 4 depicts the distribution of $\mathbf{E}$ in $\mathbf{M}$, and the grey circles represent the elements of $\mathbf{E}$.

In ECN processing, define the elements of $\mathbf{M}$ that to be moved into $\mathbf{S}$ as computational elements (CE), thus each CE has to be computed through real addition. To study the proportion $\eta_e$ of the elements of $\mathbf{E}$ in all CEs, we simulate a rate-1/2 64-ary LDPC code with length-84 symbols on BPSK-AWGN channel based on Monte Carlo method. Let $n_s = 32$, and set the maximum decoding iteration number to be 20, then the value of $\eta_e$ according to the iteration number $\text{Iter}$ is depicted in Fig. 5.

![Figure 5. The value of $\eta_e$ according to $\text{Iter}$](image)

In Figure 5, the simulating $E_b / N_0 = 2.5$ dB, and the corresponding BER $= 2.8 \times 10^{-5}$. If we consider the whole rectangular of Fig. 5 as all the CEs, then the grey region in the rectangular represents the
elements in \( \mathbf{E} \). It can be seen that, more than 75% of the CEs belong to set \( \mathbf{E} \), thus there are less than 25% of the CEs need to be computed through real additions. Therefore, the number of real additions is reduced by more than 75% in this case.

Introducing another flag variable \( F \in \{0,1\} \), the ECN processing of JD-EMS algorithm can be described as follows:

For \( k = 1 \) to \( K_{\text{max}} \) loop:

a) Extract the largest value in \( \mathbf{S} \), i.e., \( M[i,j] \). If \( M[i,j] \) has never been introduced into \( \mathbf{U}^{\mathbf{GF}} \), move \( M[i,j] \) into \( \mathbf{S} \);

b) Flag control A: if \( i = 0 \), then set \( (T = 1, \overline{T} = 0) \); if \( j = 0 \) and \( i \geq n_x - 1 \), then set \( (T = 0, \overline{T} = 1) \);

c) Flag control B: if \( M[i+\overline{T},j+T] \) has never been included in \( \mathbf{S} \), then set \( F = 0 \), else set \( F = 1 \);

d) In case \( F = 0 \), if \( M[i+\overline{T},j+T] \notin \mathbf{E} \), then compute \( V[i+\overline{T}]+I[j+T] \) and include it in \( \mathbf{S} \), else directly introduce \( M[i+\overline{T},j+T] \) in \( \mathbf{S} \) from \( \mathbf{E} \); In case \( F = 1 \), if \( M[i+\overline{T},j+T] \notin \mathbf{E} \), then compute \( V[i+\overline{T}]+I[j+T] \) and include it in \( \mathbf{S} \), else directly introduce \( M[i+\overline{T},j+T] \) in \( \mathbf{S} \) from \( \mathbf{E} \);

According to Fig. 5, it can be seen that, the proposed JD-EMS algorithm can effectively reduce the complexity of real addition operations, and similar results can be obtained on Rayleigh fading channel. Furthermore, the length of the sorter \( n_x \) can be set accurately according to (8).

5. Simulation results

By simulating a rate-1/2 64-ary LDPC code with length 84 symbols (504 bits), we examine the performances of JD-EMS algorithm, EMS algorithm as well as QSPA on BPSK-AWGN and 64-QAM Rayleigh fading channels. For brevity, EMS algorithm with parameter \( n_x = x \) is denoted as EMS(\( x \)), JD-EMS algorithm with parameter \( n_x = x \), \( n_y = y \) is denoted as JD-EMS(\( x \),\( y \)), and the maximum iteration numbers of all decoding algorithms are set to 20.

![Figure 6. Performances of QSPA, EMS and JD-EMS algorithms on BPSK-AWGN channel](image-url)
Joint Demodulation and EMS Decoding Algorithm for $Q$-ary LDPC Codes
Wei Lin, Baoming Bai, Sheng Tong
Journal of Convergence Information Technology, Volume 6, Number 6, June 2011

Figure 7. Performances of QSPA, EMS and JD-EMS algorithms on 64-QAM Rayleigh fading channel

In Figure 6, on BPSK-AWGN channel, it can be seen that the block error rate (BLER) performance of EMS(32) approaches that of QSPA, and presents no performance loss compared with QSPA at a BLER of $10^{-4}$. The BLER curve of JD-EMS(32)$_6$ nearly overlaps that of EMS(32), while JD-EMS(32)$_4$ incurs certain performance losses compared with EMS(32). It also can be seen that, EMS(16) suffers almost 0.25 dB performance loss compared with EMS(32) at BLER=$10^{-4}$, and JD-EMS(16)$_5$ performs as well as EMS(16) while EMS(16)$_3$ presents great performance loss. Therefore, for 64-ary LDPC codes over BPSK-AWGN channels, the parameters of JD-EMS algorithm can be set to $n_x = 32$, $n_b = 6$.

Figure 7 depicts the BLER performances of the decoding algorithms on 64-QAM Rayleigh fading channel, and the channel parameters are as follows: the number of paths is 64, the maximum Doppler shift is 20 Hz, and the sampling interval is 0.0005 s. It can be seen that, EMS(32) presents a performance loss of around 0.2 dB, which is acceptable on 64-QAM Rayleigh fading channel. The BLER curve of JD-EMS(32)$_5$ overlaps that of EMS(32), while JD-EMS(32)$_3$ incurs minor performance loss compared with EMS(32). EMS(16) suffers about 1 dB performance loss compared with EMS(32), and JD-EMS(16)$_4$ performs as well as EMS(16) while EMS(16)$_3$ incurs certain performance loss. Thus, for 64-ary LDPC codes over 64-QAM Rayleigh fading channels, we can choose JD-EMS(32)$_5$ or JD-EMS(16)$_3$ flexibly according to the complexity and performance requirements of the system.

5. Conclusion

A joint demodulation and EMS decoding algorithm is proposed in this paper. The proposed JD-EMS algorithm utilizes the squares of the distances between signal and constellation points over constellation graph as the decoder input soft messages, thus the complexity of computing the initial messages of the decoder can be reduced. According to the distribution of messages at ECN processing, we also improved the ECN processing in this paper, and the number of real additions can be effectively reduced. Furthermore, an upper bound of the number of comparison candidates in the sorter at each ECN step is presented, and the length of the sorter $n_b$ can be selected more accurate. Simulation results indicate that, while reducing the number of real additions at ECN processing, JD-EMS algorithm presents no performance loss compared with EMS algorithm under the corresponding parameter configurations.
6. Acknowledgement

This work was jointly supported by National Science & Technology Major Project of China under grants 2009ZX03003-011 and 2010ZX03003-003-03, the National Nature Science Foundation of China (NSFC) under grants 60972046 and 61001130.

7. References