An Improved Low-Complexity Decoding Algorithms for Non-Binary LDPC Codes in BeiDou Navigation System

Yumeng Tan1, Xiaoli Xi1,2, Hailong Yang1 and Ronghua Jiang1

1 Department of Electric Engineering, Xian University of Technology, Xian, 710048, China
2 Science and Technology on High Power Microwave Laboratory, Northwest Institute of Nuclear Technology, Xi’an 710024, China
Email: xixiaoli@xaut.edu.cn

Abstract. The construction and development of BeiDou Navigation Satellite System (BDS) is divided into three parts: BDS-1, BDS-2, and BDS-3 in sequence. The Low-Density Parity-Check (LDPC) code is applied to the BDS-3 navigation system because of its proximity to Shannon limit and the low requirement of energy. Compared with other decoding algorithms, extended Min-Sum (EMS) algorithm has been applied in navigation because it can reduce the computation of check node (CN) and facilitate hardware implementation. However, our study indicates that by calculating the correct probability of the elements in the reliability matrix, the number of candidate elements can be further reduced, thus simplifying the update of the check nodes. In this paper, an improved extended Min-Sum (IEMS) decoding algorithms is used to BDS-3 LDPC codes. Compared with the traditional EMS algorithm, the proposed decoding algorithm has the advantages of less computation and higher decoding efficiency. To verify the complexity and performance of the IEMS, the complexity and Bit Error Rate (BER) of the proposed decoding algorithm in BeiDou are studied and discussed. The simulation results show that the number of CN operations in the IEMS algorithm is only 40% times as much as that of EMS. It indicates that the IEMS decoding algorithms can be a good candidate for BDS-3 LDPC codes.

1. Introduction

In satellite navigation systems, signals are usually transmitted over a long distance and are easily disturbed and affected by noise during transmission. Therefore, the satellite signal should have as much energy as possible to ensure the reliability of the signal transmission. The signal of BDS-3 is composed of the pilot component and data component [1]. However, the pilot component will share the amount of energy of the data component, resulting in lower energy of the data component, thereby affecting the reliability of the navigation signal. To solve this problem, LDPC codes are applied in navigation systems to reduce the power loss [2]. The LDPC codes use the sparse matrix as the check matrix of the encoding and have excellent characteristics that can approximate the Shannon limit. The decoding of LDPC can be calculated in parallel, which is convenient to improve the decoding efficiency. Due to its characteristics of anti-burst error, LDPC codes have been widely used in navigation systems.

In 1962, Gallage first proposed the low-density parity-check (LDPC) code [3]. Since 1995, Mackay et al. "rediscover" LDPC codes have the capability of approaching the Shannon limit, and LDPC codes have become the focus of research in the field of channel coding [4]. Owing to its good performance, non-binary LDPC codes gradually replace binary LDPC codes in communication systems. The q-ary sum-product algorithm (QSPA) is considered to be the best non-binary LDPC decoding algorithm [5].
In [6], the extended minimum sum (EMS) method was proposed, which greatly reduced the amount of calculation. EMS decoding algorithm can reduce the computational complexity of each CN update to $O(p \log_2 n)$, where $p$ is the degree of a CN. However, the computation of the EMS on GF (q) increases with the growth of q value. In order to solve this problem, some improved decoding algorithms have been proposed, such as trellis based EMS (T-EMS) [7][8], trellis-based min-max (TMM) [9], and simplified min-sum algorithm (SMSA) [10][11]. Although these methods reduce the complexity of the EMS algorithm to some extent, there is still a large amount of computation in navigation LDPC codes. Although these algorithms reduce the complexity of codes to a certain extent, there are still some problems in BeiDou LDPC decoding, such as complex computation and large requirement of the hardware resource.

In this paper, we proposed an improved extended Min-Sum (IEMS) decoding algorithm with low-complexity in BeiDou Navigation Satellite System. The proposed IEMS decoding algorithm is simplified based on EMS algorithm, whose calculation is less reliable. EMS algorithm, as a classical decoding algorithm, has been studied and applied in both GPS and BeiDou navigation system. In order to verify the complexity and performance of the IEMS, we simulated and analysed both two algorithms taking BeiDou navigation as the research background. The simulation results show that the total computational complexity of the IEMS is only 40% of the traditional EMS algorithm, while the error performance is equivalent. The low-complexity indicates that the IEMS decoding algorithms can be a good candidate for BDS-3 LDPC decoding.

2. EMS Algorithm

This section describes the classic EMS algorithm. For regular non-binary LDPC codes, the parity check matrix has the same row weight and column weight. For the check matrix $H$ of size $m \times n$, the element of the i-th row and the j-th column is denoted as $h_{ij}$. Two index sets are given as follows:

$$M_j = \{i : 0 \leq i < m, h_{ij} \neq 0\}, 0 \leq j < n \quad (1)$$
$$N_i = \{j : 0 \leq j < n, h_{ij} \neq 0\}, 0 \leq i < m \quad (2)$$

Assume that the code word sequence $c$ after LDPC encoding is $c_j = (c_0, c_1, ..., c_{n-1})$ in GF(q), where $0 \leq j < n$. Sequence $C$ becomes a send sequence $x_j = (x_0, x_1, ..., x_{n-1})$ after BPSK modulation. By adding white Gaussian noise with a mean value of 0 and variance $\sigma^2$ to the transmitted signal, we can get the received code word $y = (y_1, y_2, ..., y_n)$, where $y_j = (y_{j,b} = B(x_{j,b}) + n_{j,b})_{b=0,1, ..., p-1}$ and $0 \leq j < N$. The log likelihood ratio (LLR) of the received message is calculated as

$$LLR(x) = \log \left( \frac{P(y_j | \hat{x}_j)}{P(y_j | x)} \right) = \frac{2 \sum_{b=0}^{p-1} y_{j,b} \Delta_{j,b}}{\sigma^2} \quad (3)$$

where $y_{j,b}$ is the bit element of each received symbol, $\Delta_{j,b} = x_{b} \ XOR \hat{x}_b$ and $\hat{x}_b = \begin{cases} 1, & x_b \geq 0 \\ 0, & x_b < 0 \end{cases}$. The EMS algorithm [6] steps are as follow:

1. Initialize: $itr = 0$. Set the maximum number of cycles to $i_{\text{max}}$.
2. Check whether $itr$ is equal to 0.
   1. Yes: Initialize the log likelihood ratio (LLR) message as $LLR$ in (3). Calculate the reliability vector $L_j = \{LLR(x), x\}$, where $x$ is the element in $GF(q)$ and $0 \leq j < N$. Initialize all $V2C_{j,\rightarrow}$ vectors of each variable node $VN_j$ as follow:
   $$V2C_{j,\rightarrow} = L_{j,\rightarrow} = L_{j,\rightarrow} \cdot h_{ij} = (x_{\rightarrow}, LLR(x_{\rightarrow})) \quad (4)$$
   2. No: Update $V2C_{j,\rightarrow}$ according to check node $C2V_{j,\rightarrow}$ as follow:
\[ V2 C_{j \rightarrow i} = h_{i,j} \cdot \left( \sum_{f \in M_{j \rightarrow i}} C2 V_{f \rightarrow j} \cdot h_{f,j}^{1} + L_{j} \right)n_{m}, 0 \leq j < n, 0 \leq i < m \]  \hspace{1cm} (5)

Generate a decision codeword as shown below:
\[ \hat{c}_{j} = \arg \min_{i \in GF(q)} \left\{ \sum_{f \in M_{j}} C2 V_{f \rightarrow j} \cdot h_{f,j}^{3} + L_{j} \right\}, 0 \leq j < n \]  \hspace{1cm} (6)

Calculate the checksum \( \hat{s} = cH^{T} \), check whether \( s \) is a zeros vector.
A. Yes: Successful decoding, exit operating.
B. No: Go to 3.

3. Update check node. Calculate the reliability vector \( C2 V_{i \rightarrow j} \) according to \( V2 C_{j \rightarrow i} \).

4. \( itr = itr + 1 \). If \( itr > i_{\text{max}} \), exit operating. Otherwise, go to 2.

Elementary Steps for check node update of the EMS algorithm (The detailed process in step 3) are as follows:

The reliability vector \( C2 V_{i \rightarrow j} \) is calculated by (7):
\[ C2 V_{i \rightarrow j} = \sum_{y \in H_{j \rightarrow i}} C2 V_{y \rightarrow i} \]  \hspace{1cm} (7)

Assume that the input vector is \((I, I), (P, P)\) and the output vector is \((Q, Q)\), where \(I, P, Q\) are \(LLR\) vectors in ascending order and \(I_{s}, P_{s}, Q_{s}\) are the corresponding Galois field element vector. Calculate the matrix \((L_{s}, L)\) of \(n_{m} \times n_{m}\) size as follow:
\[ L[r, s] = I[r] + P[s] \]  \hspace{1cm} (8)
\[ L_{j}[r, s] = I_{j}[r] \oplus P_{j}[s] \]  \hspace{1cm} (9)

The schematic diagram of the check node update is shown in Figure 1, and the update steps are as follows:

1. Store the first column of \( L \) in vector \( S \) so that \( S[\zeta] = L[\zeta, 0] \), where \( 0 \leq \zeta < n_{m} \). Set \( \varepsilon = 0 \). Set \( Q \) and \( Q_{s} \) to an empty vector.
2. Find the minimum value in vector \( S \) and mark it as \( S_{\text{min}} = L[r, s] \).
3. If \( L_{j}[r, s] \) does not exist with \( Q_{s} \), assign the minimum value of \( S \) to \( V[\varepsilon] \), assign its corresponding element to \( V_{j}[\varepsilon] \) and operate \( \varepsilon = \varepsilon + 1 \), otherwise, no action.
4. Replace \( L[r, s] \) with \( L[r, s + 1] \).
5. If \( \varepsilon \leq n_{m} \), go to 2. Otherwise, exit operating.
3. Improved EMS Algorithm (IEMS)-Low Complexity Algorithm
The algorithm procedure of IEMS algorithm is consistent with the EMS algorithm, except that the update of the check node is different. The basic step of EMS is to find the $n_m$ elements with the smallest $LLR$ value in the reliability matrix $L$ of $n_m \times n_m$ size. By analyzing the correct probability of the elements in the matrix, we can find that the elements in the first row, the first column, and $L_{n}(1,1)$ are the most reliable elements in the matrix. Therefore, we can get $n_m$ elements with the smallest $LLR$ value from $2n_m$ candidate elements. In this way, we can get an improved EMS algorithm (IEMS).

Elementary Step for check node update of the IEMS algorithm:
Assume that the input vector is $(I, I)$, $(P, P)$ and the output vector is $(Q, Q)$.

1. Calculate the value of the first column, the first row and $(1,1)$ of the matrix $L$ in (8), (9).
   Assign the first row of $L$ to $P$ and the first column of $L$ to $I$.
2. Replace $P_{n}(0,0)$ with $L_{n}(1,1)$. Then, the vector $P$ is arranged in ascending order according to the $LLR$ values corresponding to the elements.
3. By bubble check (BC) algorithm [12], select the $n_m$ elements with the smallest $LLR$ value from the vectors $P$ and take these elements as the output vector $Q$ of the basic steps. The schematic diagram of the basic steps is shown in Figure 2.

4. Simulation Results and Analysis
In this section, the numerical and experimental results of the proposed decoding algorithm are studied and discussed in BDS-3 LDPC codes, including its computational complexity and BER.

The computational complexity of CN update in per iteration of the two algorithms for the (200,100) LDPC code over $GF(64)$ are compared as follows:

| Decoding Algorithm | Galois Field Addition | Real Addition/Real comparison |
|--------------------|-----------------------|------------------------------|
| $EMS_{16}$         | 235800                | 393600                       |
| $EMS_{32}$         | 931800                | 1862400                      |
| $IEMS_{16}$        | 226200                | 39600                        |
| $IEMS_{32}$        | 912600                | 78600                        |

Figure 2. The schematic diagram of the BC Check node update.
As can be seen from Table 1, the IEMS algorithm is much less computationally intensive than the EMS algorithm. In fact, the calculation amount of $IEMS_{16}$ is about 40% of the $EMS_{16}$ algorithm.

**Figure 3.** Number of operation for real addition over GF (64).

**Figure 4.** BERs of the $(200, 100)$ code over GF(64).

**Figure 5.** BERs of the $(88, 44)$ code over GF (64).
Figure 3 shows the number of operation for real addition over $GF(64)$. It can be seen in Figure 3 that with the increase of $n_m$, the computation of EMS algorithm increases greatly, while the IEMS algorithm grows slowly. Compared with the traditional EMS algorithm, the computational complexity and the computational speed of the proposed IEMS algorithm are significantly improved. In order to compare the decoding performance of the two methods, we simulated the LDPC codes with different code lengths under two BDS3 frequencies in B2A and B1C, respectively. Figure 4 shows that, for the (200,100) LDPC code over $GF(64)$ in the B2A signal, the $IEMS_{16}$ algorithm performs within 0.25dB from the $EMS_{16}$ algorithm at the BER of $10^{-6}$. It indicates that the IEMS algorithm can still maintain good decoding efficiency in the case of reduced computational complexity. Figure 5 shows that the IEMS algorithm can still maintain a good decoding performance with a shorter code length in the B1C signal.

5. Conclusion
In this paper, the low-complexity improved EMS decoding algorithm is applied to the BeiDou Navigation Satellite System. Compared with the traditional EMS algorithm, the total computational complexity of the proposed IEMS algorithm is only 40% of the EMS algorithm. In addition, to verify the performance of the IEMS algorithm, both the LDPC codes of B2A and B1C of the BDS-3 are simulated and studied. The simulated results verified the proposed algorithm has lower complexity and better decoding efficiency in BDS-3 LDPC codes. Good performance of the IEMS algorithm proved that it can be a good candidate for BDS-3 LDPC codes.

6. Acknowledgments
This work was supported in part by Key research and development plan of Shaanxi Province (2017ZDXM-GY-117), National Defense Pre-Research Foundation of China (6140450010302).

7. References
[1] BeiDou Navigation Satellite System Signal In Space Interface Control Document," (1.0) Beijing China 2013.
[2] R. Qian, P. Ying and W. Liu. Research on the Coding of Beidou Satellite Navigation Signal Based on Quasi-Cyclic LDPC code [DB/OL]. The 4th China Satellite Navigation Conference.
[3] Gallage. Low-Density Parity-Check Codes. IRE Trans.Inform.Theory. 1962, 1(8): 21-28.
[4] Mackay. Near-Shannon-limit-performance-of-low-density-parity-check-codes. 1995
[5] M. C. Davey and D. MacKay, “Low-density parity check codes over $GF(q)$,” IEEE Commun. Lett., 1998, 2(6): 165–167.
[6] A. Voicila, D. Declercq, F. Verdier, et al. Low-complexity decoding for non-binary LDPC codes in high order fields[J]. IEEE Transactions on Communications, 2010,58(5):1365-1375.
[7] E. Li, D. Declercq and K.Gunnam, “Trellis-based extended min-sum algorithm for non-binary LDPC codes and its hardware structure,” IEEE Trans. Commun., 2013, 61 (7): 2600–2611.
[8] J. Lacruz, F. Garcia-Herrero, J. Valls and D. Declercq, “One minimum only trellis decoder for non-binary low-density paritycheck codes,” IEEE Trans. Circuits Syst. I, Reg. Papers, 2015, 62 (1): 177–184.
[9] J. Lacruz, F. Garcia-Herrero, D. Declercq and J. Valls, “Simplified trellis min–max decoder architecture for non-binary low-density parity check codes,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 2015, 23(9): 1783–1792.
[10] L. Song, Q. Huang, and Z. Wang, “Set min-sum decoding algorithm for non-binary LDPC codes,” in Proc. IEEE Int. Symp. Inf. Theory, 2016: 3008–3012.
[11] C. Wang, X. Chen, Z. Li and S. Yang, “A simplified min-sum decoding algorithm for non-binary LDPC codes,” IEEE Trans. Commun., 2013, 61(1): 24–32.
[12] E. Boutillon and L. Conde-Canencia, “Bubble check: a simplified algorithm for elementary check node processing in extended min-sum non-binary LDPC decoders”, Elect. Lett., 2010, 46(9): 633–634.