International Journal of Information Engineering and Applications
2018; 1(3): 104-117
http://www.aascit.org/journal/information

AASCIT American Association for Science and Technology

Binary and Non-Binary Low Density Parity Check Codes: A Survey

Salah Abdulghani Alabady

College of Engineering, Computer Engineering Department, University of Mosul, Mosul, Iraq

Email address

eng.salah@uomosul.edu.iq

Citation

Salah Abdulghani Alabady. Binary and Non-Binary Low Density Parity Check Codes: A Survey. *International Journal of Information Engineering and Applications*. Vol. 1, No. 3, 2018, pp. 104-117.

Received: March 23, 2018; **Accepted**: April 9, 2018; **Published**: May 31, 2018

Abstract: Forward error detection and correction codes have been widely either used of storage applications or transferred through a wireline or wireless communication media systems for many years. Due to the unreliable wireless links, broadcast nature of wireless transmissions, interference, moreover, noisy transmission channel, frequent topology changes, and the various quality of wireless channel, there are challenge to provide high data rate service, high throughput, high packet delivery ratio (PDR), low end-to-end delay and reliable services. In order to address these challenges, several channel coding scheme are proposed. In this paper, detailed overviews of the major concepts in error detection and correction codes are presented. The paper provided fundamentals of Low Density Parity Check (LDPC) codes, and a comprehensive survey of the binary and non-binary LDPC codes is provided.

Keywords: Hamming, RS, LDPC, Detection and Correction Codes

1. Introduction

During the past decade, many schemes have been proposed to increase the reliability of the wireless network and communication systems, in order to fulfill the quality of the data in a high data rate wireless network applications, such as telephone conversations, video conference and television cameras. In wireless networks and wireless digital communication applications, channel coding have received considerable attention, since some data bits might be exposed to attenuation or distortion due to interferences, channel noise and multi-path fading. In addition, both random and burst errors occur during transmission in noisy communication channel. These types of errors increase the bit-error-rate (BER) which results in bad quality transmission. Channel coding is considered one of the major boosts, which enhances the performance of wireless networks at higher data rates. In wireless network applications and real time application systems, low complexity and shorter codeword length in channel coding scheme are preferred. Channel coding is used for point-to-point communication over a single channel, and it uses the error correction coding to improve the error performance of the wireless link. It is implemented at the physical layer to recover erroneous bits through redundant parity check bits added inside a packet. The error retrieval capability for channel coding depends on the specific coding and the amount of redundant bits.

Transmissions in the wireless networks are jeopardized by the injection of errors or erasure of symbols data. Errors are caused by the channel noise or by the multi-path fading channel. Recently, Low Density Parity-Check (LDPC) codes [1] have been extensively developed and regarded as the best channel coding schemes. The error correction capability of the LDPC codes depends on the codeword length and the characteristic of the parity check matrix H [1-2]. The decoder gives a better performance with a larger codeword (i.e. large size of G matrix) and with good parity-check matrix H. In practice, to achieve a better BER performance with LDPC codes close to the channel capacity, the length of the LDPC codeword used should be in the order of thousands of bits [1]. The LDPC decoding is effective only when the parity-check matrix has a relatively large column weight [3]. The matrix multiplication for this big codeword size demands huge memory, computational requirements and more complex decoding [4, 5, 2]. Consequently, the existing decoding algorithms are either too costly to implement [6]. Furthermore, LDPC codes require iteration in the detection and correction error processes around 10 to 50 times of iteration [7]. For example, the average number of iterations for iterative decoding of the LDPC (1008, 504) code with belief

propagation (BP) and uniformly most powerful (UMP) BP-based decoding algorithms, is 50 and 200 [8]. Besides, the decoder fails to correct errors if the number of errors occurred is greater than the error correction capability of the decoder regardless of the number of iterations [2]. For practical applications, these codes are inappropriate to be used since they involve high encoding-decoding complexity. Therefore, the need of efficient channel codes with lower encoding and decoding complexity, and lower memory size requirement, which do not require any iteration in the decoding process, is quite obvious.

2. Background

This section provides background of basic concepts of the channel coding such as, Hamming, RS, and LDPC codes. Nowadays, wireless networks applications and digital communication have become part of day-to-day life. Robust wireless data transmissions are taken for granted. Any real wireless communication system is plague by errors that occur from time to time in data transmissions and from many different sources such as random noise, interference, channel fading, etc. Reliable data transmissions would be impossible without the use of error control techniques. Error detection and correction especially in a high reliability and high data rate wireless network applications have been receiving considerable attention and have been become an important part of networking and data communications. Best networks must be able to transfer data from source to destination or from one node to another node with complete accuracy and reliability. Using the error detection and correction techniques improves the network performance in terms of enhanced throughput, decrease in BER and reduction of end-to-end delay. Therefore, there is requirement to research in the area of coding theory to design codes for channels that are power and bandwidth limited.

Different types of channel coding (error correction coding), along with their properties are reviewed. Fundamentals, concept, and types of network coding are introduced. This chapter also introduces the concept of joint network with channel coding schemes and the benefits of this joint. The second part of this chapter contains the review of related works in error correction codes, specific for low density parity check (LDPC) code. In addition, literature review of wireless network coding and joint network with channel coding is presented.

Normally, there are two strategies to combat the errors namely stand alone and combined. The first one is the automatic repeat request (ARQ) [9-10]. The ARQ retransmission method is often implemented because it is very simple to use in many actual networks. ARQ used with error detection and not error correction system, as correction is much harder. The basic idea is that if any errors are found, the receiver notifies the transmitter of the existence of errors. The transmitter then resends the data until they are correctly received. In general, the codes used with ARQ are CRC (Cyclic Redundancy Checks) [11]. Such systems provide reliable transmission for networks.

The second strategy, known as the forward error correction (FEC), not only detects but also corrects the errors, so that data retransmission can be avoided. In many practical applications retransmission may be difficult or not even feasible at all. The retransmission becomes more critical in real time applications, such as video conference and remote control in wireless sensor network (WSN) that depends on live broadcast. In this case, FEC is the only practical solution. The common feature of communication channel is that information emanates from a source and is sent over the channel to a receiver at the other end. The channel in noisy in the sense that what is received is not always the same as what was sent. Thus if binary data is being transmitted over the channel, when a 0 is sent, it is hopefully received as a 0 but sometimes will be received as a 1 (or as unrecognizable). The fundamental problem in coding theory is to determine what message was sent on the basis of what is received.

3. Channel Coding Overview

Channel coding is an error-control technique used to provide robust data transmission through imperfect channels by adding redundancy to the data. There are two important classes of channel coding methods namely, block, and convolutional coding. In information and coding theory, error detection and correction are techniques which enable the reliable delivery of digital data over unreliable communication channels [11]. Error detection and correction especially in a high reliability and high data rate wireless network applications have been receiving considerable attention and have become an important part of networking and data communications. Best networks communication must be able to transfer data from source to destination or from one node to another node with complete accuracy and reliability. Therefore, for reliable networks, it is desirable to detect and correct the error at the destination node without need to send a retransmit request again to the sender node. By using the error detection and correction techniques the network performance will improve by increasing the throughput and PDR, and decreasing the BER and end-to-end delay.

The use of error correction, however, is not free. The redundancy acts as overhead and it costs the transmission resources (e.g., channel bandwidth or transmission power). Therefore, the redundancy is better to be as small as possible. A quantitative measure of the redundancy is the coding rate *Rc* which is defined as the ratio of the message length k to the codeword length n as shown in Eq. 1

$$R_c = \frac{k}{n} \tag{1}$$

The maximum value of R_c is 1 when no redundancy is added (i.e., when the information is uncoded). Coding performance and coding rate are two opposing factors. When more redundancy is added, the error correction capability is strengthened, but the coding rate drops [12].

3.1. Types of Channel Coding

Depending on how redundancy is added, there are two families of codes, namely block codes and convolutional codes. Block coding encodes and decodes data on a block by-block basis. In this case, data blocks are independent from each other. Block codes denoted by (n, k), k is the message length, n is the codeword length and $r = n - k$ is the parity bits or check bits. A Generator Matrix **G** (of order $k \times n$) is used to generate the code. In contrast, the convolutional codes work on a continuous data stream and their encoding and decoding operations depend not only on the current data but also on the previous data. The general construction of G matrix is shown in Eq. (2)

$$\mathrm{G} = [\mathrm{I_k\ P}]_{k \times n} \tag{2}$$

where, I_k is the $k \times k$ identity matrix and P is a $k \times (n - k)$ matrix selected to give desirable properties to the code produced.

In addition, there are systematic and nonsystematic codes. When the redundancy is explicitly appended to the message, the code is systematic. On the other hand, if the redundancy is implicitly embedded in the codeword, the code is said to be nonsystematic. Systematic codes are always preferred in practice, because the message and the parity are separated; in this case, the receiver can directly extract the message from the decoded codeword. The proposed code namely low complexity parity check (LCPC).

3.2. Considerations of Selecting the Channel Code Scheme

Selecting channel-coding scheme for a practical application is not an easy task. In fact, many factors it needs to take into account: error detection and correction capability, decoding complexity, error types, signal power constraints and processing latency. However, no single channel coding scheme works for all applications. In Shannon's theorem, the longer the code, the better the error correcting performance. On the other hand, longer code means higher decoding complexity and larger processing latency. The decoding process dominates the overall computational cost of an error control system. In real time application, large amounts of latency are not preferred. Therefore, we have to make a trade-off between the performance and complexity when selecting the channel code scheme. The ensemble average bound on uncorrected error probability can give us an estimate of how the performance and the complexity are related. For block codes of length n and coding rate R_c, the bound P_E is:

$$P_E \leq 2^{-nE_B(R_c)} \tag{3}$$

Where, $E_B(R_c)$ is positive function of R_c and is completely determined by the channel characteristics.

In addition, the type of errors encountered during data transmission is another important consideration. There are two types of errors, random errors and busty errors. Random errors affect the data independently. Busty errors are contiguous. An error control code must match the error type in order to be effective. Most codes are designed to combat random errors; only a few codes such as Reed-Solomon codes are good for correcting burst errors. With redundancy added, the coding rate $R_c = k/n$ be comes less than unity and the effective data rate is reduced. To maintain the same data rate, we need to raise the overall throughput. An increase in throughput translates into more channel bandwidth.

3.3. Hamming Codes

Hamming codes are one of binary linear block error-correcting codes that were proposed by Hamming [13]. Hamming codes provide single bit error correction and double bit error detection. The parameters for Hamming codes for any positive integer $m \geq 3$ are $n = 2^m - 1$, $k = n - m$ and $d_{min} = 3$ [14]. Hamming codes are able to protect four bit information (data bits) from a single error in a codeword by adding three redundant bits to the data bits. The generator matrix G and the parity check matric H for Hamming (7, 4) code are shown in Eq. 4 and Eq. 5 respectively [2].

In Hamming (7, 4) code, a message that has four data bits is transmitted as a 7-bit codeword by adding three error control bits. The three bits to be added are three even parity bits.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \tag{4}$$

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{5}$$

The inability of Hamming code for not being able to correct double bit error can be attributed to the limited number of syndrome. In Hamming code (7, 4), the H matrix consists of 3 rows and 7 columns which account for 8 values of syndrome vector [15]. In case of single bit error, there are 7 possibilities of error pattern when the codeword length is 7 bits. In this case, each error pattern is assigned one syndrome vector. In case of double bit errors, there are 21 possibilities of error pattern, and the Hamming code does not have this number of syndromes (i.e., 21). Hamming code (7, 4) only has 8 syndrome vector (i.e., 2^m) and $m = 3$. Therefore, in case of double bit error, each 2 or 3 error patterns are assigned one syndrome vector. This makes the correct operation difficult and impossible because it cannot precisely detect the correct error pattern from the 2 or 3 error patterns. In addition, Hamming code cannot detect more than two bit errors (e.g., burst error) [15, 16].

The minimum Hamming distance is defined as $d_{min} = n$-k, where $n = 7$ is the codeword length and $k = 4$ is the message length, and $d_{min} = 3$. The number of errors that a block code can detect and correct is determined by its minimum Hamming distance d_{min}. This is defined as the minimum number of places where any two codewords vary. In general, the number of errors u that can be detected for a block code is $u = d_{min} - 1$. For example, at $m = 3$, the codeword length $n = 7$, message length $k = 4$ and $d_{min} = 3$. Where, t is the number of

errors that a block code can correct as shown in Eq. 6. Since, the Hamming code has a minimum Hamming distance $d_{min} = 3$; it can only correct one bit error for each 7 bits transmitted. Therefore, the percentage of error correction is (1/7= 14.285%).

$$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1 \quad (6)$$

3.4. Reed Solomon (RS) Codes

Reed Solomon (RS) [17] codes are one of the block error correcting codes, used in a wide range of digital communication and data storage applications. RS codes are the subset and the extension of the nonbinary Bose Chaudhuri and Hocquenghem (BCH) codes as well as linear block codes, as in the same way the BCH codes are extension of the Hamming codes [18]. RS codes are a good kind of channel coding techniques used for correcting a burst error in the fading channel and suitable for data block transmission. A particular RS code is specified as RS (*n, k*) with *s*-bit symbols, where *n* is the code length and *k* is the length of the data word. This means that the encoder takes *k* data symbols of *s* bits each and adds parity symbols to make an $n = 2^s - 1$ symbol codeword. There are (*n-k*) parity symbols of s bits each. The minimum distance of RS codes is ($n - k + 1$). The number and type of errors that can be corrected in RS code depends on the characteristics of that code [11], [17]. An RS decoder can correct up to t symbols that contain errors in a 20 codeword, where $2t = n - k$. To increase the capability of error correction, the number of the parity code must increase. This means, the value of *t* in RS code must be large.

If $s = 3$, n is 7, and when the number of parity is 3, k is 4. The maximum number of symbols errors that can be corrected by RS code is *t*, which is given by, $t = \lfloor (n-k)/2 \rfloor$.

So, based on *t* value the RS (7, 4) code can correct only one symbol error from the 7 codeword symbols that are transmitted. When the symbol size is 3, the worst case happens when only one bit error occurs in separate symbols. In this case the error correction is 1/21× 100 = 4.7619%. This value is small compared to the percentage of error correction in Hamming (7, 4) code, and this explains why the Hamming (7, 4) code has better BER performance compared to the RS (7, 4) code. The best case for RS (7, 4) code occurs when there are only all bits in a one symbol is errors. This means the percentage of error correction is the number of errors in one symbol over the total number of symbols bit transmitted (i.e. 3/21 = 14.285%).

Therefore to increase the capability of error correction, the value of t in RS code must be large, which means that the number of the parity code must increase, leading to increased complexity in encoding and decoding processes.

As an example: A popular Reed-Solomon code is RS (255, 223) with 8-bit symbols. Each block contains 255 codeword bytes (2040 bits), of which 223 bytes are data and 32 bytes are parity. For this code: $n = 255$, $k = 223$, $s = 8$, $2t = 32$, and $t = 16$.

A large value of *t* means that a large number of errors can be corrected, but it requires more computing power than a small value of *t* and increases complexity. One 21-symbol error occurs when 1 bit in a symbol is wrong or when all the bits in a symbol are wrong. RS (255, 223) decoder can correct 16 symbol errors. The worst case occurred when 16 bit errors might occur, and each one of these bits is in a separate symbol (byte), so that the decoder could correct a maximum of 16 bit errors from the 2040 bits (255×8). The percentage of error correction is (16/2040 = 0.784%). The best case occurred when complete 16 byte errors happened so that the decoder could correct 128 bit (16×8) errors from the 2040 bits. The percentage of error correction is 128/2040 = 6.274%. Thus, there is limitation in the number of errors that the decoder can correct errors in each block. This limitation depends on the number of parity bytes. RS codes are particularly suited to correcting burst error (where a series of bit errors in the received codeword). In addition, RS algebraic decoding procedures can correct errors and erasures. An erasure occurs when the position of an error symbol knows. A decoder can correct up to t errors or up to 2*t* erasures.

RS codes are based on a special area of mathematics known as Galois fields or finite fields. A finite field has the property that arithmetic operations ($+, -, \div, \times$) on the field elements always have a result in the field. An RS encoder or decoder needs to carry out these arithmetic operations. The codeword in RS codes is generated using a special polynomial. All valid code words are exactly divisible by the generator polynomial. The general form of the generator polynomial is:

$$g(x) = (x - a^1)(x - a^{i+1}) \ldots\ldots (x - a^{1+2t}) \quad (7)$$

The codeword is constructed by using:

$$c(x) = g(x) \times m(x) \quad (8)$$

where, $g(x)$ is the generator polynomial, $m(x)$ is the information block, $c(x)$ is a valid codeword.

3.5. Low Density Parity Check (LDPC) Codes

One of the leading families of error-correcting codes is known as Low-Density Parity-Check (LDPC) codes which were first developed in 1963 by Gallager [1], [19] and revived by Mackay and Neal 20 in 1996 [20]. An LDPC code can be described by specifying its parity check matrix H, which is an $m \times n$ binary matrix. The name "low density" refers to the fact that the matrix H is very sparse [21]. The LDPC code, also known as the Gallager code, was invented in 1962 [19]. LDPC was the first error correcting code that allowed data transmission rates close to the theoretical maximum the Shannon limit [20], and this existed only for long code lengths (at least a few thousands of bits). The LDPC code was ignored since its introduction, owing to its difficulty in implementation largely because its decoding complexity exceeded the hardware capacity.

In 1990s, Mackay and Neal rediscovered the code [22]. Basically, there are two different possibilities to represent LDPC codes. Like all linear block codes they can be described via matrices. The second possibility is a graphical representation. The matrix defined in Eq. 9 [23], [24] is a parity check matrix with dimension $m \times n$ for a (8, 4) code,

w_r for the number of 1's in each row and w_c for the number of 1's in each column. For the matrix to be called low density the two conditions $w_c \leq m$ and $w_r \leq n$ must be satisfied. In order to do this, the parity check matrix should usually be very large. The LDPC code is regular if w_c is constant for every column and w_r is constant for every row. On the other hand, if w_c and w_r are not constants, the LDPC code is irregular. In general, the BER performance of irregular LDPC codes are better than those of regular LDPC codes by up to 0.5 dB [25], [12]. Eq. 9 is an example of the H matrix for regular LDPC code since it contains two 1's per column and four 1's per row for all columns and rows. Figure 1 is a Tanner graph that represents the H matrix for regular LDPC (8, 4) code, where $w_c = 2$ and $w_r = 4$ as shown in Eq. 9 [23].

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (9)$$

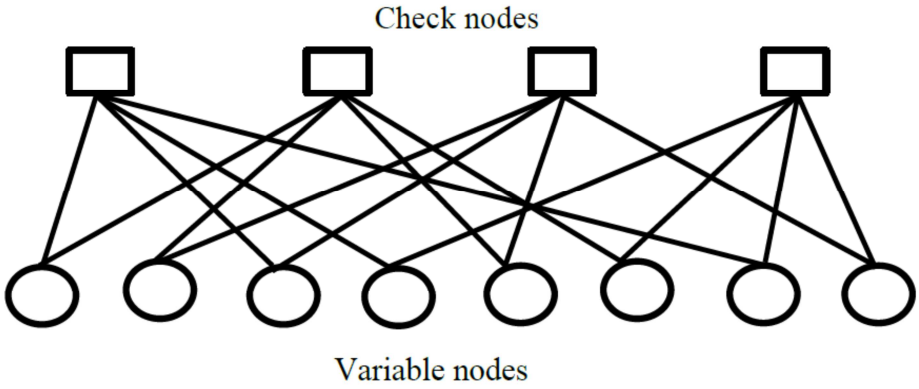

Figure 1. *Tanner graph of LDPC (8, 4) code.*

The error correction capability of LDPC code also depends on the codeword length and the characteristic of the parity check matrix. The decoder gives a better performance with a larger codeword (i.e., big size of G matrix) and with good parity-check matrix [2]. In practice, to achieve a better BER performance with LDPC codes close to the channel capacity, the length of the LDPC codeword used should be in the order of thousands of bits. For example, the simulation results show that to obtained a BER of 10^{-6} within 0.04 dB of the Shannon limit, a block length of 10^7 is needed [26]. The matrix multiplication for that big codeword size demands huge memory, computational requirements and more complex decoding. Besides, the decoder fails to correct errors if the number of errors occurred is greater than the error correction capability of the decoder regardless of the number of iterations. On the contrary, our proposed low complexity parity check (LCPC) codes give a good BER performance with small codeword and this is one advantage of LCPC codes.

To verify codeword, LDPC code uses a large binary parity-check matrix H. Each row and column of H will have a predetermined number of ones, which is designed to be a very low fraction of the total number of elements. The rows correspond to parity-checks on those bits and the columns of H correspond to the bits of the received message. In practice, to achieve a better BER performance with LDPC codes and close to the channel capacity, the codeword length of the LDPC used is in the order of thousands of bits. In addition, a good LDPC code should possess a large minimum distance d_{min} and no short cycles in its Tanner graph. The matrix multiplication for that big code word size demands huge memory, computational requirements and more complexity to the decoding. However, this is considered as one of the disadvantages of LDPC codes. In any way, the decoder fails to correct errors if the number of errors occurred is greater than the error correction capability of the decoder regardless of the number of iterations.

The disadvantages of the LDPC codes include higher encoding complexity, longer latency than turbo code, and poor performance compared to turbo codes when code length is short [12]. LDPC code has been adopted in several standards including IEEE 802.16 (WiMAX) [27], IEEE 802.3 (10G Base-T Ethernt) [28] and DVB-S2 (satellite transmission of digital television) [29], [30]. The algorithm to decode LDPC codes is available in different names; the most common are belief propagation algorithm, message passing algorithm and sum-product algorithm.

4. Encoding and Decoding Algorithms of LDPC Codes

Compared to others types of error correction codes, the encoding algorithm of LDPC poses a challenge [12] because the generator matrix G of an LDPC code is usually not sparse. In addition, due to the large size of the matrix, the conventional block encoding method could require a significant number of computations. For example, the G matrix of LDPC codes for a code rate 0.5 with codeword length of 8,000 bits and the message length of 4,000 is a matrix of (4,000 × 8,000). The encoding process (i.e., multiplication of the G matrix with the message) requires 10^7 XORs (i.e., more complexity) even if we assume the density of the matrix to be as low as 0.2 [12]. The complexity of encoders and decoders grows rapidly as the code length increases.

LDPC decoding adopts an iterative approach. The LDPC decoding operates alternatively on the bit nodes and the check nodes to find the most likely codeword c that satisfies the condition $cH^T = 0$. Several decoding algorithms exist for LDPC codes. For hard-decision decoding, there is the bit-flipping (BF) algorithm [31-33]; for soft-decision decoding, there is the sum-product algorithm (SPA) [34-37], also known as the belief propagation algorithm [4] and message passing algorithm [38-40]. To obtain convergence to true optimum iterative soft-decision decoding of LDPC, Tanner graph should not contains cycles or contains a few cycles as possible. Tanner graph of proposed LCPC codes no contains cycles and this is one advantage of LCPC codes.

There are two types of LDPC codes depending on the properties of the G and H matrices elements. These types are binary and non-binary LDPC codes. A non-binary LDPC code is simply an LDPC code with a sparse parity check matrix containing elements that could be defined over finite fields GF (2^i), where i is a positive integer greater than 1. Davey and MacKay [41] presented the idea of LDPC codes over finite fields, proving that they could achieve enhanced performance over their binary counterparts with increasing finite field size. Mackay also showed how the sum-product algorithm could be extended to decode non-binary LDPC codes, but the overall complexity was much higher. Therefore (during that time), the decoding of non-binary LDPC codes was restricted over small finite fields.

LDPC codes became very popular in several applications such as the digital satellite broadcasting system (DVB-S2), Wireless Local Area Network WLAN (IEEE 802.11n) and WiMAX (802.16e) [42]. LDPC codes are widely used in recent research for their excellent performance and ability to perform very close to the Shannon capacity limit [20]. However, there are some challenging issues in their implementation: how to design an LDPC code in the case of a finite block length, and how to reduce the complexity in encoding and decoding, storing the parity check matrix and reducing the longer latency and the number of iteration [43]. Belief propagation algorithm and min-sum algorithm are two major decoding algorithms used in LDPC codes [22].

Four classes of geometric approach to the construction of LDPC codes are constructed based on the lines and points of Euclidean and projective geometries over finite fields by [4]. Codes of these four classes have good minimum distances and their Tanner graphs [44] have girth 6. The advantage of finite-geometry LDPC codes can be decoded in different ways, ranging from low to high decoding complexity and from reasonably good to very good performance. These decoding methods include Gallager's bit flipping (BF) decoding [1], one-step majority-logic (MLG) decoding [11], weighted MLG decoding [45], weighted BF decoding, a posteriori probability (APP) decoding [19] and iterative decoding based on belief propagation (commonly known as sum-product algorithm (SPA)) [22, 8, 46-48]. They perform will be very well with iterative decoding. Moreover, they can be put in either cyclic or quasi-cyclic form [4]. The performance of the LDPC codes over finite fields GF(q) is better than the binary LDPC, at short and medium block lengths. Nonetheless, the decoder of LDPC GF(q) has more complexity [49].

Two types of LDPC codes, Binary and Non-Binary LDPC codes [50-52]. Binary LDPC (B-LDPC) codes show good error correction capability and channel capacity utilization for large block lengths. The short codeword lengths exhibit poorer performance [53] because of short cycles in parity matrix. Non-binary LDPC (NB-LDPC) codes are defined in Galois field GF (q), i.e. the elements of the field are 0, 1,...., q-1. NB-LDPC codes were found to have better performance than binary codes at short and medium codeword lengths. However, higher the order of the field better is the performance at the cost of encoder/hardware complexity.

4.1. Binary LDPC Codes

Binary LDPC (B-LDPC) codes show excellent error correction capability and channel capacity utilization for large block lengths. For short codeword lengths they exhibit poorer performance due to short cycles in parity matrix [53]. B-LDPC codes, are discovered by Gallager in 1962 [19], who proposed the bit flipping (BF) decoding and one-step majority-logic (OSMLG) decoding algorithms [1]. Mackay [20] have rediscovered the performance of LDPC on Gaussian channels. They studied the theoretical and practical properties of BF and min-sum algorithms of LDPC. Mackay has shown the LDPC approaching Shannon limit in long code length [20]. Since their rediscovery, a great deal of research has been conducted in the study of code construction methods, decoding techniques, and performance analysis. Fossorier et al. [8] proposed two simplified versions of the belief propagation algorithm for fast iterative decoding of LDPC codes on the AWGN channel. These two algorithms do not require any knowledge about the channel characteristics. With hardware-efficient decoding algorithms such as the min-sum algorithm, practical decoders can be implemented for effective error control. Therefore, binary LDPC codes have been considered for a wide range of applications such as satellite broadcasting, wireless communication, optical communication, and high density storage systems. Kim et al. [43] proposed binary LDPC code structure using cyclic shift matrices and an efficient LDPC code construction algorithm using the characteristic matrix to achieve fast construction time, low encoding complexity and reduced memory.

Luby et al. [25] presented an improvement in Gallager's results by introducing irregular parity-check matrices and a new rigorous analysis of hard-decision decoding of these codes. Also, an efficient method for finding good irregular structures for such decoding algorithms was shown. Richardson and Urbanke [47] presented a general method for determining the capacity of LDPC codes. This method was implemented under message-passing decoding when used over any binary-input memory less channel with discrete or continuous output alphabets. Kou et al. [4] presented four classes of LDPC codes constructed based on the lines and points of Euclidean and projective geometries over finite fields.

Kim et al. [43] proposed an LDPC code structure using

cyclic shift matrices and an efficient LDPC code construction algorithm using the characteristic matrix. The number of rows (column) in the characteristic matrix was B times smaller than those in the parity check matrix. They demonstrated that the construction time required for the proposed LDPC code is much smaller than that required for a conventional LDPC code with the same codeword length and code rate. In addition, the proposed LDPC code can achieve those improvements in complexity without performance degradation. Zhong and Zhang [23] proposed a block-LDPC design approach that joint LDPC code encoder-decoder for practical LDPC coding system. Miladinovic and Fossorier [31] presented a proposed decoding algorithm for improving the hard-decision bit-flipping decoding for LDPC codes. The authors have been shown that the proposed decoding algorithm provides slows down the decoding in the case of an ideal code whose bipartite graph has a tree structure, with no performance gain to be expected.

A class of message-passing decoders for LDPC codes was proposed by Ardakani et al., [54] who proved that, if the channel is symmetric and all codewords are equally likely to be transmitted, an optimum decoding rule should satisfy certain symmetry and isotropy conditions. The simulation results showed that algorithm B, in the case of regular codes, was the optimum binary message-passing algorithm in the sense of minimizing message error rate. In addition, algorithm B remained optimum in the case of irregular codes, if the variable nodes did not exploit structural knowledge of their local decoding neighborhood. In addition, they found a bound on the achievable rates with Gallager's Algorithm B. An improved bit-flipping decoding algorithm for high-rate Finite-Geometry Low Density Parity-Check (FG-LDPC) codes is proposed [55]. The improvement in performance and decrease in decoding delay were observed by flipping multiple bits in each iteration. The results showed that the proposed algorithm achieved a tradeoff between performance and complexity for FG-LDPC codes. In addition, a modification of Improved Weighted Bit Flipping (IWBF) was proposed. The modified algorithm was called Multiple Bit-Flipping (MBF) which could update multiple bits in each iteration. This modification led to improvement in performance in terms of both the Bit-Error Rate (BER) and Frame-Error Rate (FER), and drastically speeded up the decoding process.

Irregular LDPC codes using Belief Propagation (BP) decoding algorithm for Binary Input Additive White Gaussian Noise (BIAWGN) channel is designed [56]. The knowledge of the Signal-to-Noise Ratio (SNR) at the receiver is required to achieve ultimate performance in the case of BP algorithm over BIAWGN channel. An erroneous estimation of the SNR at the decoder is referred to as SNR mismatch. The irregular LDPC codes performed better in the presence of mismatch compared to the conventional irregular LDPC codes that are optimized for zero mismatches.

In addition, the designed code showed good performance even outside the mismatch range of interest. Chilappagari and Vasic [57] investigated the error-correction capability of column weight three LDPC codes when decoded using the Gallager A algorithm and extended the results to the bit flipping algorithms. A necessary condition for a code to correct all error patterns with up to $k \geq 5$ errors was provided to avoid cycles of length up to $2k$ in its Tanner graph and proved that a code with a Tanner graph of girth $g \geq 10$ cannot correct all error patterns with up to $g/2$ errors. This result settled the problem of error-correction capability of column-weight-three LDPC codes [57].

Oh and Parhi [58] proposed improved normalized min-sum (MS) decoding algorithm and novel MS decoder architectures with reduced codeword length using nonuniform quantization schemes for LDPC codes. The proposed algorithm introduced a more exact adjustment with two optimized correction factors for check-node-updating computations, whereas the conventional normalized MS algorithm applies only one correction factor. In addition, the proposed nonuniform quantization scheme could reduce the finite word length while achieving similar performances compared to a conventional quantization scheme and provided a significant performance gain without any additional computation or hardware complexity. The simulation results showed that the proposed 4-bit nonuniform quantization scheme achieved an acceptable decoding performance unlike the conventional 4-bit uniform quantization schemes. Sassatelli and Declercq [59] have introduced a new class of LDPC codes, named hybrid LDPC codes. Hybrid LDPC codes are characterized by an irregular connectivity profile and heterogeneous orders of the symbols in the codeword. The class of hybrid LDPC codes can be asymptotically characterized and optimized using density evolution (DE) framework, and a technique to maximize the minimum distance of the code is presented. Hybrid LDPC codes are allowed to achieve an interesting trade-off between good error-floor performance and good waterfall region with non-binary coding techniques.

An implementation-friendly binary message-passing decoding method for time invariant decoding for LDPC codes that do not require the degree information of variable nodes or degree dependent parameters is introduced [60]. An estimation and analysis methods for the extrinsic error probability (EEP) and code optimizations for the proposed time invariant decoder were developed. The proposed method offered similar performance as the existing methods for time-invariant decoding in most cases, while it facilitated efficient circuit implementations of the LDPC decoder. Table 1 summarizes the related works in binary LDPC codes. Belean et al. [61] have proposed FPGA hardware architectures approach implementation for short length LDPC decoders based in the belief propagation and minsum algorithms. The LDPC decoder implementation is suitable for applications that use short-length LDPC codes, due to its parallel computation capabilities.

In [62], the authors proposed a blind binary LDPC encoder identification scheme for M-quadrature amplitude modulation (M-QAM) signals. To estimate the unknown signal amplitude, noise variance, and phase offset for M-QAM signals, the expectation maximization (EM) algorithm is developed. In addition, the authors investigated the average iteration number

needed for the EM algorithm to converge for different modulation orders. An iterative reliability-based modified majority-logic decoding algorithm for two classes of structured low-density parity-check codes is presented [63]. To recover the performance degradation that caused by the simply flipping operation, the authors design a turbo-like iterative strategy. In [64], exact density evolution of LDPC codes over the Binary Erasure Channel (BEC) is presented. The authors derived and expressed upper bounds on the threshold by bounding multivariate evolution functions as single-variable minimizations. In [65], a new method for decoding of LDPC codes over the AWGN channel is proposed. The proposed method is applied using a standard belief-propagation (BP) decoder followed by list erasure decoder. The performance of the proposed method is analyzed mathematically and demonstrated by simulations.

The authors in [66] presented a novel method of low-complexity near-maximum likelihood (ML) decoding of quasi-cyclic (QC) LDPC codes over the binary erasure channel. ML decoding is applied to a relatively short window which is cyclically shifted along the received sequence. The idea is similar to wrap-around decoding of tail-biting convolutional codes. A method for distributed source coding, using LDPC codes to compress close to the Slepian-Wolf limit for correlated binary sources is proposed [67]. A conventional BP algorithm LDPC decoder is developed which considers the syndrome information. In [68] the authors proposed a method called the parallel vector message passing-based edge exchange (PMPE), for optimizing a type of graph-based LDPC codes, without changing the code length, code rate and degree distribution. The authors have been proposed the optimization method, which can increase the Hamming distance of the LDPC codes. In addition, the optimization method for quasi-cyclic (QC) LDPC codes called the parallel vector message passing oriented-to the QC-LDPC codes (QC-PMP) is suggested. Xuan He et al., [69] propose a new multi-edge metric-constrained for progressive edge-growth (PEG) algorithm (MM-PEGA) to improve the design for binary LDPC code at each variable node. The authors analyzed the properties of the multi-edge local girth, and proposed an algorithm for calculating the multi-edge local girth.

Table 1. *Chronology of research activities on Binary-LDPC.*

Reference	Summary of work performed
(R. Gallager, 1963)	First discovered binary low-density parity-check (B-LDPC) codes with the bit flipping (BF) decoding and one-step majority-logic (MLG) decoding algorithms.
(MacKay and Neal, 1996; MacKay, 1999)	Rediscovered and studied the performance of LDPC on Gaussian channels. Studied the theoretical and practical properties of belief propagation algorithm, and min-sum algorithms of LDPC codes. It was shown that LDPC approached Shannon limit in long code length.
(M. P. C. Fossorier, M. Mihaljevic, and H. Imai, 1999)	Two simplified versions of the belief propagation algorithm for fast iterative decoding of LDPC codes on the AWGN channel were proposed. These two algorithms do not require any knowledge about the channel characteristics.
(M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, 2001)	An improvement in Gallager results by introducing irregular parity-check matrices was reported and a new rigorous analysis of hard-decision decoding of these codes was presented. Also, an efficient method for finding good irregular structures for such decoding algorithms was shown.
(T. J. Richardson and R. L. Urbanke, 2001)	A general method for determining the capacity of LDPC codes was presented. This method was implemented under message-passing decoding when used over any binary-input memory less channel with discrete or continuous output alphabets.
(Y. Kou, S. Lin, and M. P. C. Fossorier, 2001)	Four classes of LDPC codes constructed based on the lines and points of Euclidean and projective geometries over finite fields, were presented.
(K. S. Kim, S. H. Lee, Y. H. Kim, and J. Y. Ahn, 2004)	An LDPC code structure using cyclic shift matrices and an efficient LDPC code construction algorithm using the characteristic matrix was proposed. Simulation results showed that the construction time required for the proposed LDPC code was much smaller than that required for a conventional LDPC code with the same codeword length and code rate.
(H. Zhong and T. Zhang, 2005)	Block-LDPC design approach that joint low-density parity-check (LDPC) code-encoder-decoder was proposed for practical LDPC coding system.
(N. Miladinovic and M. P. C. Fossorier, 2005)	The authors presented a proposed decoding algorithm for improving the hard-decision bit-flipping decoding for LDPC codes. The authors have been shown that the proposed decoding algorithm slows down the decoding in the case of an ideal code whose bipartite graph has a tree structure.
(M. Ardakani and F. R. Kschischang, 2005)	A class of message-passing decoders for LDPC codes was presented. The authors proved that, if the channel is symmetric, all codewords are equally likely to be transmitted. In addition, they found a bound on the achievable rates with Gallager Algorithm B.
(M. Ardakani and F. R. Kschischang, 2006)	A class of iterative message-passing decoders for LDPC codes was considered which where the decoder could choose its decoding rule from a set of decoding algorithms at each iteration.
(T. M. N. Ngatched, F. Takawira, and M. Bossert, 2009)	An improved bit-flipping decoding algorithm for high-rate finite-geometry low-density parity-check (FG-LDPC) codes was proposed. The improvement in performance and decrease in decoding delay were observed by flipping multiple bits in each iteration.
(H. Saeedi and A. H. Banihashemi, 2009)	A Belief propagation (BP) algorithm for decoding LDPC codes over a binary input additive white Gaussian noise (BIAWGN) channel was designed. To achieve ultimate performance, the algorithm requires the knowledge of the SNR at the receiver.
(S. K. Chilappagari and B. Vasic, 2009)	The error-correction capability of column-weight-three LDPC codes was investigated when decoded used the Gallager A algorithm.
(D. Oh and K. K. Parhi, 2010)	An improvement of the normalized min-sum (MS) decoding algorithm and novel MS decoder architectures with reduced word length using nonuniform quantization schemes for LDPC codes were proposed.
(L. Sassatelli and D. Declercq, 2010)	A new class of LDPC codes, named hybrid LDPC codes, was introduced. Asymptotic analysis of this class of codes was carried out for distribution optimization, as well as finite-length optimization.

Reference	Summary of work performed
(G. S. Yue and X. D. Wang, 2010)	An implementation-friendly binary message-passing decoding method for time invariant decoding for LDPC codes was introduced that does not require the degree information of variable nodes or degree dependent parameters.
(B. Belean, S. Nedevschi, and M. Borda, 2013)	FPGA hardware architectures approach implementation for short length LDPC decoders based in the belief propagation and min-sum algorithms is proposed. The proposed architecture achieves high throughput in real time application.
(T. Xia, H.-C. Wu, S. Y. Chang, X. Liu, and S. C.-H. Huang, 2014)	A blind binary LDPC encoder identification scheme for M- quadrature amplitude modulation (M-QAM) signals proposed. Expectation maximization (EM) algorithm is used to estimate the unknown signal amplitude, noise variance, and phase offset for M-QAM signals.
(H. Chen, L. Luo, Y. Sun, X. Li, H. Wan, and L. Luo, 2015)	An iterative reliability-based modified majority-logic decoding algorithm for two classes of structured low-density parity-check codes is presented.
(S. Harikumar, J. Ramesh, M. Srinivasan, and A. Thangaraj, 2015)	Protograph LDPC codes are optimized for good thresholds using a closed-form upper bound on threshold. The results show that a simple randomized construction optiend in small-sized protographs with threshold close to capacity upper bounds.
(I. E. Bocharova, B. D. Kudryashov, V. Skachek, and Y. Yakimenka, 2016)	The authors proposed a new method for decoding of LDPC codes over the AWGN channel using a standard belief-propagation (BP) decoder that followed by list erasure decoder.
(I. E. Bocharova, B. D. Kudryashov, E. Rosnes, V. Skachek, and O. Ytrehus, 2016)	Presented a novel method of low-complexity near-maximum likelihood (ML) decoding of quasi-cyclic (QC) LDPC codes over the binary erasure channel. The authors are studied by simulations a few examples of regular and irregular QC LOPC codes, and the performance is compared with the ensemble-average performance.
(S. Eleruja, U.-F. Abdu-Aguye, M. Ambroze, M. Tomlinson, and M. Zak, 2017)	Propose a scheme for distributed source coding, using LDPC codes to compress close to the Slepian-Wolf limit for correlated binary sources. In addtation, the authors developed a conventional BP algorithm LDPC decoder which takes the syndrome information into account.
(X. Liu, F. Xiong, Z. Wang, and S. Liang, 2017)	Proposed two optimization methods, the PMPE algorithm for random codes and the QC-PMP algorithm for QC-LDPC codes. The proposed algorithms can decrease the number of short cycles in the Tanner graphs without changing the code parameters such as the code length, code rate and degree distribution.
(X. He, L. Zhou, and J. Du, 2018)	The authors proposed depth-first search (DFS)-like algorithm to calculate the multi-edge local girth. In addition, the set based method (SBM) has been proposed to replace the breadth-first search (BFS)-like method so as to accelerate the multi-edge metric-constrained PEG algorithm (MM-PEGA). Moreover, the MM-PEGA has been generalized for improving different PEG-like designs.

4.2. Non-Binary LDPC Codes

Davey and MacKay [41] are the first who investigated non-binary LDPC (NBLDPC) codes over the Galois field of order q which is known as q-ary LDPC codes. NB-LDPC codes are considered as the extension of the B-LDPC codes. Davey and MacKay extended the sum-product algorithm (SPA) for B-LDPC codes to decode qary LDPC codes and referred to this extension as the q-ary SPA (QSPA). NB-LDPC codes over the Galois field GF(q), was viewed as an extension of BLDPC codes. Davey and MacKay are the first who investigated NB-LDPC. The entries in the parity-check matrix of an NB-LDPC code belong to GF(q) ($q > 2$). NB-LDPC codes are defined in Galois field GF(q) where q is the field size ($q > 2$). Barnault and Declercq [70] presented a modification of Belief Propagation scheme. The modification scheme enabled to decode LDPC codes defined on high order Galois fields with a complexity that was scaled as $p\log2(p)$, p being the field order. The low complexity algorithm had the ability to decode GF(2^q) LDPC codes up to a field order value of 256. Simulation result exhibited very good performance that ultra-sparse regular LDPC codes in GF(64) and GF(256).

Wymeersch et al. [71] introduced a log-domain decoding scheme for LDPC codes over GF (q). The scheme was mathematically equivalent to the conventional sum-product decoder. The log-domain decoding had advantages in terms of implementation, computational complexity and numerical stability. Additionally, a suboptimal variant of the log-domain decoding algorithm was proposed, yielding a lower computational complexity. The log-SPA decoding scheme for general NB-LDPC codes based on LLRs was derived. The proposed log-domain version (log-SPA) and a sub-optimal implementation (max log-SPA) algorithms and the SPA were compared in terms of both simulated BER performance and computational complexity. As log-domain SPA and SPA are mathematically equivalent, they have identical BER performance. Maxlog SPA gives rise to a small BER degradation (about 0.5 dB).

Voicila et al. [5] presented a new implementation of the EMS decoder for NBLDPC codes using log-density-ratio as messages. The new algorithm has taken into account the memory problem of the NB-LDPC decoders and decoding complexity. The implementation of the EMS decoder reduced the order of complexity to $O(n_m \log_2 n_m)$, with $n_m << q$; this complexity was smaller than the complexity of the BP-FFT decoder. The low complexity and low memory of EMS decoding algorithm render it as a good candidate for the hardware implementation of NB-LDPC decoders. The EMS decoding algorithm could approach the performance of the BP decoder and even in some cases beat the BP decoder. However, higher order of the field size provides better performance, but the cost of encoder and hardware complexity increase. The two low-complexity reliability algorithms based message-passing algorithms for decoding LDPC codes over non-binary finite fields is presented [72]. First one is called One Step Majority-logic decoding (OSMLGD) algorithm and the second is Iterative hard reliability based (IHRB)-MLGD algorithm. The authors have been shown that the decoding algorithms provide effective trade-off between error performance and decoding complexity compared to the non-binary sum product algorithm.

Aruna and Anbuselvi [73] have presented the Fast Fourier Transform-Sum product algorithm (FFT-SPA) based NB-LDPC codes for various order of Galois Field with

different parity check matrices (PCM) structures. The decoding performance is analyzed for the specification of IEEE 802.11n standard. The authors have proposed two modified parity check matrices (PCM) to reduce the computation strength. The first one is lower diagonal based PCM (LDM) and the second is doubly diagonal based PCM (DDM). Wang et al. [74] presented a new decoding algorithm for the NB-LDPC decoder based on the q-ary min-sum algorithm (QMSA). The new algorithm modified the check node (CN) computations of the QMSA into two steps. By reorganizing the message entries and providing the most likely symbol, a compressed intermediate message could be easily obtained and stored, from which the check-to-variable messages could be computed with a look-up table. The authors proposed two simplified variants based on QMSA for practical designs: first one is the extended min-sum algorithm (EMSA) working with message truncation and sorting to reduce complexity and memory requirements; second one is the Min-Max algorithm (MMA) [75], which replaces the sum operations in the check node processing by max operations. Simulation results demonstrated that the proposed algorithm had negligible performance loss compared to the QMSA, over AWGN channel.

Wang et al. [76] presented a hardware-efficient NB-LDPC decoding algorithm codes, called the simplified min-sum algorithm SMSA, which had reduced-complexity decoding algorithm. The simulation results demonstrated that the proposed scheme had small performance loss over the additive white Gaussian noise channel and independent Rayleigh fading channel. Furthermore, the proposed hardware scheme had reduced complexity; a good performance-complexity tradeoff could be efficiently implemented. Based on the analysis results, the SMSA had much lower complexity and lower memory usage compared to other decoding algorithms for NB-LDPC codes. Lin and Yan [77] proposed a simplified decoding algorithm to reduce computational complexities of variable node processing for NB-LDPC codes over large fields. An improved based check node processing algorithm for NB-LDPC codes was proposed to reduce the memory requirement. The reduced memory requirement was due to truncating the message vectors to a limited number (n_m) of values. However, the memory requirements of these decoders remained high when the field size was large, since (n_m) needs to be large enough to alleviate error performance degradation.

In addition, a priori message compression algorithm was proposed to reduce memory consumption. Numerical results showed that the proposed decoding algorithm outperformed the existing algorithms. However, the NB-LDPC codes outperformed their binary counterparts in some cases, but their high decoding complexity was a significant hurdle to their applications [49, 77]. Bhargava and Bose [3] applied a Sum Product Algorithm (SPA) for decoding of NB-LDPC codes. They showed that SPA had better performance than B-LDPC code of equivalent length. Both the memory complexity and latency are high for the forward-backward (FB) approach when the check node degree is high [77]. The FB approach is widely used in check node processing (CNP) [75].

The authors in [78] proposed two flexible and simple methods for constructing non-binary (NB) quasi-cyclic (QC) LDPC codes. The proposed construction methods have several known ingredients including base array, masking, binary to non-binary replacement and matrix-dispersion. In addition, a reduced-complexity iterative decoding scheme for NB-CPM-QC-LDPC codes, called MGRD-scheme is presented. In [79] a non-binary LDPC codes for the erasure channel, under maximum a posteriori decoding is proposed. The authors presented a design method for finite-length q-aryLDPC codes on the q-EC under MAP decoding. L. Dolecek et al. [80], provided a comprehensive analysis of non-binary (LDPC) codes. The authors considered both random and constrained edge weight labeling, and refer to the former as the unconstrained nonbinary protograph-based LDPC codes (U-NBPB codes). In [81], the computational complexity of check node update in the extended Min-Sum (EMS) algorithm is reduced by set partition. The authors in [82], proposed a method to reduce the computational complexity of NB-LDPC decoding using modulation assisted preprocessing scheme.

Two methods are proposed in [83] to improve the iterative hard-reliability based majority-logic decoding (IHRBMLGD) algorithm for NB-LDPC codes. The first method improves the error-correcting performance by modifying the initialization process, which is because Gray coded modulation is used in general. The second method is the storage reduction method that is proposed to reduce the memory size considerably while sustaining the error-correcting performance achieved by the modified initialization. A LDPC coded modulation approach addressing orthogonal modulations is proposed in [84] over the AWGN channel with moderate order between 8 and 32. The proposed design is based on a constrained EXIT-based optimization of a NB-LDPC ensemble degree distribution, where the restriction lies in the search of degree distributions that lead to low error floors. The authors in [85] studied the Gallager ensembles of binary regular LDPC codes and binary images of nonbinary regular LDPC code.

Table 2. *Chronology of research activities on Non-Binary LDPC.*

Reference	Summary of work performed
(M. C. Davey and D. J. MacKay, 1998)	The empirical results of error-correction using the analogous codes over GF(q) for $q > 2$ with binary symmetric channels and binary Gaussian channels were introduced. There was significant improvement over the performance of the binary codes, including a rate 1/4 code with BER < 10-5 at Eb/No = 0.2 dB.
(L. Barnault and D. Declercq, 2003)	A modification of Belief Propagation scheme was presented. The modification scheme enabled to decode LDPC codes defined on high order Galois fields with a complexity that was scaled as p log2 (p), p being the field order.
(H. Wymeersch, H. Steendam, and M.	A log-domain decoding scheme for LDPC codes over GF (q) was introduced. The scheme is mathematically

Moeneclaey, 2004)	equivalent to the conventional sum-product decoder. The log-domain decoding has advantages in terms of implementation, computational complexity and numerical stability. The log-SPA decoding scheme for general non-binary LDPC codes based on LLRs was derived.
(A. Voicila, D. Declereq, F. Verdier, M. Fossorier, and P. Urard, 2007)	A new implementation of the EMS decoder for non-binary LDPC codes was presented using log-density-ratio as messages. The implementation of the EMS decoder reduced the order of complexity to $O(n_m \log_2 n_m)$, with $n_m << q$; this complexity is smaller than the complexity of the BP-FFT decoder.
(D. Declercq and M. Fossorier, 2007)	In this work, the problem of decoding NB-LDPC codes over finite fields GF(q) is introduced address, with a simplified decoder called extended min-sum (EMS).
(L. Chun-Hao, W. Chien-Yi, L. Chun-Hao, and C. Tzi-Dar, 2008)	In this work, the log-domain decoder for non-binary LDPC over GF(q) is presents. The proposed decoder can efficiently reduce the decoding complexity to $O(q\log q)$.
(C.-Y. Chen, Q. Huang, C.-c. Chao, and S. Lin, 2010)	The authors have presented a new two low-complexity decoding algorithms (OSMLGD and IHRB-MLGD) for LDPC codes over the non-binary finite fields.
(C.-L. Wang, Z. Li, and S. Yang, 2012)	A new decoding algorithm for the NB-LDPC decoder based on the q-ary min-sum algorithm (QMSA) was presented. The new algorithm modified the check node (CN) computations of the QMSA into two steps. Simulation results demonstrated that the proposed algorithm had negligible performance loss compared to the QMSA over AWGN channel.
(S. Aruna and M. Anbuselvi, 2013)	Two modified parity check matrices (LDM and DDM) based on the PCM are proposed to reduce the computation strength of NB-LDPC. FFT-SPA algorithm based NB-LDPC codes for various order of GF is presented.
(J. Wang, X. Liu, K. Chi, and X. Zhao, 2013)	A hardware-efficient NB-LDPC decoding algorithm codes, called the simplified min-sum algorithm SMSA was presented, which reduced-complexity decoding algorithm. The simulation results demonstrated that the proposed scheme had small performance loss over the additive white Gaussian noise channel and independent Rayleigh fading channel.
(J. Lin and Z. Yan, 2013)	A simplified decoding algorithm to reduce computational complexities of variable node processing for NB-LDPC codes over large fields was proposed. An improved based check node-processing algorithm for NB-LDPC codes was proposed to reduce the memory requirement. The reduction in memory was achieved by truncating the message vectors to a limited number nm of values.
(L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri,, 2014)	A class of structured non-binary LDPC codes built out of protographs, called NBPB codes. The authors considered both constrained and unconstrained edge weight selections.
(J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, 2015)	Two simple and flexible methods for constructing NB-QC-LDPC codes with CPM structure are proposed from a matrix-theoretic point of view. The proposed methods are very effective for constructing codes of short to long block lengths and low to high rates.
(G. Garrammone, E. Paolini, B. Matuz, and G. Liva, 2015)	Propsosed a NB-LDPC codes for the erasure channel, under maximum a posteriori decoding. The authors presented a design method for finite-length q-aryLDPC codes on the q-EC under MAP decoding and provided Monte Carlo simulation results for several short non-binary LDPC codes.
(L. Song, Q. Huang, and Z. Wang, 2016)	The complexity of decoding NB-LDPC codes is reduced by set partition. The input vectors in the check node are partitioned into several sets such that different elements in the virtual matrix enjoy various computational strategies.
(T. Wu, H.-C. Yang, and J. Yan, 2016)	Proposed a modulation assisted preprocessing scheme to reduce the computational complexity of NB-LDPC decoding.
(S. Yeo and I.-C. Park, 2017)	Improve the iterative hard-reliability based majority-logic decoding (IHRBMLGD) algorithm for NB-LDPC codes using two methods. The first one improves the error-correcting performance. The second one is proposed to reduce the memory size considerably.
(G. Liva, B. Matuz, E. Paolini, and M. F. Flanagan, 2017)	Proposed a NB-LDPC coded modulation approach addressing orthogonal modulations over the AWGN channel with moderate order.

5. Conclusion

Error correcting code is a necessity in any network communication system, and it is the commonly used in modern telecommunications technique in order to increase the reliability of a data transfer. There are many types of error-correcting codes. One of the leading families of error-correcting codes is known as Low-Density Parity-Check (LDPC) codes. In this paper, a detailed of the major concepts in error correction coding was presented. Chronology of research activities on Binary LDPC Non-Binary LDPC is provided.

References

[1] R. Gallager, "Low density parity check codes, number 21 in Research monograph series," MIT Press, Cambridge, Mass, 1963.

[2] R. A. Carrasco, and M. Johnston, *Non-Binary Error Control Coding for Wireless Communication and Data Storage*: Wiley Publishing, 2009.

[3] L. Bhargava, and R. Bose, "Novel hardware implementation of LLR-based non-binary LDPC decoders," in IEEE National Conference on Communications (NCC), 2013, pp. 1-5.

[4] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Transactions on Information Theory,* vol. 47, no. 7, pp. 2711-2736, 2001.

[5] A. Voicila, D. Declereq, F. Verdier, M. Fossorier, and P. Urard, "Low-complexity, low-memory EMS algorithm for non-binary LDPC codes," in IEEE International Conference on Communications, ICC'07, 2007, pp. 671-676.

[6] C. L. Wang, X. H. Chen, Z. W. Li, and S. H. Yang, "A Simplified Min-Sum Decoding Algorithm for Non-Binary LDPC Codes," *IEEE transactions on communications,* vol. 61, no. 1, pp. 24-32, 2013.

[7] A. Salbiyono, and T. Adiono, "LDPC decoder performance under different number of iterations in mobile WiMax," in International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2010, pp. 1-4.

[8] M. P. C. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE transactions on communications,* vol. 47, no. 5, pp. 673-680, 1999.

[9] D. Yang, and W. C. Lee, "Adaptive Hybrid Automatic Repeat Request (ARQ) with a Novel Packet Reuse Scheme for Wireless Communications," in The 9th International Conference on Advanced Communication Technology, Okamoto, Kobe, Japan, 2007, pp. 597-601.

[10] D. J. Claypool, and K. M. McNeill, "Automatic repeat request (ARQ) over TDMA-based mesh network," in IEEE Military Communications Conference (MILCOM 2008), San Diego, CA, USA, 2008, pp. 1-7.

[11] S. Lin, and D. J. Costello, *Error control coding: fundamentals and applications*: Pearson Education India, 2004.

[12] Y. Jiang, *A practical guide to error-control coding using MATLAB*: Artech House, 2010.

[13] R. W. Hamming, "Error detecting and error correcting codes," *Bell System technical journal,* vol. 29, no. 2, pp. 147-160, 1950.

[14] T. K. Moon, *Error correction coding*: Wiley Online Library, 2005.

[15] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*: Wiley-Interscience, 2005.

[16] S. B. Wicker, *Error control systems for digital communication and storage*: Prentice-Hall, Inc., 1994.

[17] I. S. Reed, and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial & Applied Mathematics,* vol. 8, no. 2, pp. 300-304, 1960.

[18] B. Sklar, and F. J. Harris, "The ABCs of linear block codes," *IEEE Signal Processing Magazine,* vol. 21, pp. 14-35, 2004.

[19] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory,* vol. 8, no. 1, pp. 21-28, 1962.

[20] D. J. MacKay, and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electronics letters,* vol. 32, no. 18, pp. 1645, 1996.

[21] J. Campello, D. S. Modha, and S. Rajagopalan, "Designing LDPC codes using bit-filling." pp. 55-59.

[22] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory,* vol. 45, no. 2, pp. 399-431, Mar, 1999.

[23] H. Zhong, and T. Zhang, "Block-LDPC: A practical LDPC coding system design approach," *IEEE Transactions on Circuits and Systems I-Regular Papers,* vol. 52, no. 4, pp. 766-775, Apr, 2005.

[24] L. Chun-Hao, W. Chien-Yi, L. Chun-Hao, and C. Tzi-Dar, "An O(qlogq) Log-Domain Decoder for Non-Binary LDPC Over GF(q)," in IEEE Asia Pacific Conference on Circuits and Systems, (APCCAS), 2008, pp. 1644-1647.

[25] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Transactions on Information Theory,* vol. 47, no. 2, pp. 585-598, 2001.

[26] B. M. Leiner, *LDPC Codes–a brief Tutorial*, 2005.

[27] Y.-L. Wang, Y.-L. Ueng, C.-L. Peng, and C.-J. Yang, "Processing-Task Arrangement for a Low-Complexity Full-Mode WiMAX LDPC Codec," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 58, no. 2, pp. 415-428, 2011.

[28] A. E. Cohen, and K. K. Parhi, "A Low-Complexity Hybrid LDPC Code Encoder for IEEE 802.3an (10GBase-T) Ethernet," *Ieee Transactions on Signal Processing,* vol. 57, no. 10, pp. 4085-4094, 2009.

[29] G. Falcao, J. Andrade, V. Silva, and L. Sousa, "Real-time DVB-S2 LDPC decoding on many-core GPU accelerators." in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2011, pp. 1685-1688.

[30] S.-M. Kim, C.-S. Park, and S.-Y. Hwang, "A novel partially parallel architecture for high-throughput LDPC Decoder for DVB-S2," *IEEE Transactions on Consumer Electronics,* vol. 56, no. 2, pp. 820-825, 2010.

[31] N. Miladinovic, and M. P. C. Fossorier, "Improved bit-flipping decoding of low-density parity-check codes," *IEEE Transactions on Information Theory,* vol. 51, no. 4, pp. 1594-1606, 2005.

[32] S. A. Muaini, A. Al-Dweik, and M. Al-Qutayri, "BER performance of turbo product LDPC codes with non-sequential decoding," in 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC), 2013, pp. 1-6.

[33] T. C. Chen, "Channel-independent weighted bit-flipping decoding algorithm for low-density parity-check codes," *IET Communications,* vol. 6, no. 17, pp. 2968-2973, 2012.

[34] L. Safarnejad, and M. R. Sadeghi, "FFT Based Sum-Product Algorithm for Decoding LDPC Lattices," *IEEE Communications Letters,* vol. 16, no. 9, pp. 1504-1507, 2012.

[35] M. Johnston, B. S. Sharif, C. C. Tsimenidis, and L. Chen, "Sum-Product Algorithm Utilizing Soft Distances on Additive Impulsive Noise Channels," *IEEE Transactions on Communications,* vol. 61, no. 6, pp. 2113-2116, 2013.

[36] N. Noorshams, and M. J. Wainwright, "Stochastic Belief Propagation: A Low-Complexity Alternative to the Sum-Product Algorithm," *IEEE Transactions on Information Theory,* vol. 59, no. 4, pp. 1981-2000, 2013.

[37] W. Li, Z. Yang, and H. Hu, "Sequential Particle-Based Sum-Product Algorithm for Distributed Inference in Wireless Sensor Networks," *IEEE Transactions on Vehicular Technology,* vol. 62, no. 1, pp. 341-348, 2013.

[38] M. Karimi, and A. H. Banihashemi, "Message-Passing Algorithms for Counting Short Cycles in a Graph," *IEEE Transactions on Communications,* vol. 61, no. 2, pp. 485-495, 2013.

[39] N. Ruozzi, and S. Tatikonda, "Message-Passing Algorithms: Reparameterizations and Splittings," *IEEE Transactions on Information Theory,* vol. 59, no. 9, pp. 5860-5881, Sep, 2013.

[40] S. H. Lee, M. Shamaiah, H. Vikalo, and S. Vishwanath, "Message-Passing Algorithms for Coordinated Spectrum Sensing in Cognitive Radio Networks," *IEEE Communications Letters,* vol. 17, no. 4, pp. 812-815, 2013.

[41] M. C. Davey, and D. J. MacKay, "Low density parity check codes over GF (q)," in Information Theory Workshop, 1998, pp. 70-71.

[42] G. Falcao, V. Silva, J. Marinho, and L. Sousa, "LDPC Decoders for the WiMAX (IEEE 802.16 e) based on Multicore Architectures," in WIMAX New Developments, Upena D Dalal and Y P Kosta (Ed.) 2009.

[43] K. S. Kim, S. H. Lee, Y. H. Kim, and J. Y. Ahn, "Design of binary LDPC code using cyclic shift matrices," *Electronics letters,* vol. 40, no. 5, pp. 325-326, 2004.

[44] R. M. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Transactions on Information Theory,* vol. 27, no. 5, pp. 533-547, 1981.

[45] V. D. Kolesnik, "Probabilistic decoding of majority codes," *Problemy Peredachi Informatsii,* vol. 7, no. 3, pp. 3-12, 1971.

[46] R. Lucas, M. P. Fossorier, Y. Kou, and S. Lin, "Iterative decoding of one-step majority logic deductible codes based on belief propagation," *IEEE Transactions on Communications,,* vol. 48, no. 6, pp. 931-937, 2000.

[47] T. J. Richardson, and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Transactions on Information Theory,* vol. 47, no. 2, pp. 599-618, 2001.

[48] F. R. Kschischang, B. J. Frey, and H. A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on Information Theory,* vol. 47, no. 2, pp. 498-519, 2001.

[49] X. Chen, and A. Men, "Reduced complexity and improved performance decoding algorithm for nonbinary LDPC codes over GF (q)," in 11th IEEE International Conference on Communication Technology, (ICCT) 2008, pp. 406-409.

[50] S. M. Song, B. Zbou, S. Lin, and K. Abdel-Ghaffar, "A Unified Approach to the Construction of Binary and Nonbinary Quasi-Cyclic LDPC Codes Based on Finite Fields," *IEEE Transactions on Communications,* vol. 57, no. 1, pp. 84-93, 2009.

[51] G. J. Han, and X. C. Liu, "A Unified Early Stopping Criterion for Binary and Nonbinary LDPC Codes Based on Check-Sum Variation Patterns," *IEEE Communications Letters,* vol. 14, no. 11, pp. 1053-1055, 2010.

[52] P. Venkateshwari, and M. Anbuselvi, "Decoding performance of binary and non-binary LDPC codes for IEEE 802.11 n standard," in IEEE International Conference on Recent Trends In Information Technology (ICRTIT), 2012, pp. 292-296.

[53] S. Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Communications Letters,* vol. 5, no. 2, pp. 58-60, 2001.

[54] M. Ardakani, and F. R. Kschischang, "Properties of optimum binary message-passing decoders," *IEEE Transactions on Information Theory,* vol. 51, no. 10, pp. 3658-3665, 2005.

[55] T. M. N. Ngatched, F. Takawira, and M. Bossert, "An Improved Decoding Algorithm for Finite-Geometry LDPC Codes," *IEEE Transactions on Communications,* vol. 57, no. 2, pp. 302-306, 2009.

[56] H. Saeedi, and A. H. Banihashemi, "Design of Irregular LDPC Codes for BIAWGN Channels with SNR Mismatch," *IEEE Transactions on Communications,* vol. 57, no. 1, pp. 6-11, 2009.

[57] S. K. Chilappagari, and B. Vasic, "Error-Correction Capability of Column-Weight-Three LDPC Codes," *IEEE Transactions on Information Theory,* vol. 55, no. 5, pp. 2055-2061, 2009.

[58] D. Oh, and K. K. Parhi, "Min-Sum Decoder Architectures With Reduced Word Length for LDPC Codes," *Ieee Transactions on Circuits and Systems I-Regular Papers,* vol. 57, no. 1, pp. 105-115, 2010.

[59] L. Sassatelli, and D. Declercq, "Nonbinary Hybrid LDPC Codes," *IEEE Transactions on Information Theory,* vol. 56, no. 10, pp. 5314-5334, 2010.

[60] G. S. Yue, and X. D. Wang, "An Implementation-Friendly Binary LDPC Decoding Algorithm," *IEEE Transactions on Communications,* vol. 58, no. 1, pp. 95-100, 2010.

[61] B. Belean, S. Nedevschi, and M. Borda, "Application specific hardware architecture for high-throughput short-length LDPC decoders," in IEEE International Conference on Intelligent Computer Communication and Processing (ICCP), 2013, pp. 307-310.

[62] T. Xia, H.-C. Wu, S. Y. Chang, X. Liu, and S. C.-H. Huang, "Blind identification of binary LDPC codes for M-QAM signals." in IEEE Global Communications Conference (GLOBECOM), 2014, pp. 3532-3536.

[63] H. Chen, L. Luo, Y. Sun, X. Li, H. Wan, L. Luo, and T. Qin, "Iterative reliability-based modified majority-logic decoding for structured binary LDPC codes," *Journal of Communications and Networks,* vol. 17, no. 4, pp. 339-345, 2015.

[64] S. Harikumar, J. Ramesh, M. Srinivasan, and A. Thangaraj, "Threshold upper bounds and optimized design of protograph LDPC codes for the Binary Erasure Channel." in Seventh International Workshop on Signal Design and its Applications in Communications (IWSDA), 2015, pp. 186-190.

[65] I. E. Bocharova, B. D. Kudryashov, V. Skachek, and Y. Yakimenka, "Low complexity algorithm approaching the ML decoding of binary LDPC codes." in IEEE International Symposium on Information Theory (ISIT), 2016, pp. 2704-2708.

[66] I. E. Bocharova, B. D. Kudryashov, E. Rosnes, V. Skachek, and O. Ytrehus, "Wrap-around sliding-window near-ML decoding of binary LDPC codes over the BEC." in 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC), 2016, pp. 16-20.

[67] S. Eleruja, U.-F. Abdu-Aguye, M. Ambroze, M. Tomlinson, and M. Zak, "Design of binary LDPC codes for Slepian-Wolf coding of correlated information sources." in IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2017, pp. 1120-1124.

[68] X. Liu, F. Xiong, Z. Wang, and S. Liang, "Design of Binary LDPC Codes with Parallel Vector Message Passing," *IEEE Transactions on Communications*, 2017.

[69] X. He, L. Zhou, and J. Du, "A New Multi-Edge Metric-Constrained PEG Algorithm for Designing Binary LDPC Code With Improved Cycle-Structure," *IEEE Transactions on Communications,* vol. 66, no. 1, pp. 14-25, 2018.

[70] L. Barnault, and D. Declercq, "Fast decoding algorithm for LDPC over GF (2q)," in Information Theory Workshop, 2003, pp. 70-73.

[71] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over GF (q)," in IEEE International Conference on Communications, 2004, pp. 772-776.

[72] C.-Y. Chen, Q. Huang, C.-c. Chao, and S. Lin, "Two low-complexity reliability-based message-passing algorithms for decoding non-binary LDPC codes," *IEEE Transactions on Communications,* vol. 58, no. 11, pp. 3140-3147, 2010.

[73] S. Aruna, and M. Anbuselvi, "FFT-SPA based non-binary LDPC decoder for IEEE 802.11n standard," in International Conference on Communications and Signal Processing (ICCSP), 2013, pp. 566-569.

[74] C.-L. Wang, Z. Li, and S. Yang, "A new min-sum based decoding algorithm for non-binary LDPC codes," in International Conference on Computing, Networking and Communications (ICNC), 2012, pp. 476-480.

[75] V. Savin, "Min-Max decoding for non binary LDPC codes," in IEEE International Symposium on Information Theory (ISIT), 2008, pp. 960-964.

[76] J. Wang, X. Liu, K. Chi, and X. Zhao, "Complex field network-coded cooperation based on multi-user detection in wireless networks," *Journal of Systems Engineering and Electronics,* vol. 24, no. 2, pp. 215-221, 2013.

[77] J. Lin, and Z. Yan, "A decoding algorithm with reduced complexity for non-binary LDPC codes over large fields," in IEEE International Symposium on Circuits and Systems (ISCAS), 2013, pp. 1688-1691.

[78] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "A matrix-theoretic approach to the construction of non-binary quasi-cyclic LDPC codes," *IEEE Transactions on Communications,* vol. 63, no. 4, pp. 1057-1068, 2015.

[79] G. Garrammone, E. Paolini, B. Matuz, and G. Liva, "Non-binary LDPC erasure codes with separated low-degree variable nodes," *IEEE Transactions on Communications,* vol. 63, no. 11, pp. 3937-3949, 2015.

[80] L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri, "Non-binary protograph-based LDPC codes: Enumerators, analysis, and designs," *IEEE Transactions on Information Theory,* vol. 60, no. 7, pp. 3913-3941, 2014.

[81] L. Song, Q. Huang, and Z. Wang, "Set min-sum decoding algorithm for non-binary LDPC codes." in IEEE International Symposium on Information Theory (ISIT), 2016, pp. 3008-3012.

[82] T. Wu, H.-C. Yang, and J. Yan, "Modulation assisted preprocessing for non-binary LDPC decoding with extended min-sum algorithm." in IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2016, pp. 1-4.

[83] S. Yeo, and I.-C. Park, "Improved Hard-Reliability Based Majority-Logic Decoding for Non-Binary LDPC Codes," *IEEE Communications Letters,* vol. 21, no. 2, pp. 230-233, 2017.

[84] G. Liva, B. Matuz, E. Paolini, and M. F. Flanagan, "Non-binary LDPC codes for orthogonal modulations: Analysis and code design." in IEEE International Conference on Communications (ICC), 2017, pp. 1-6.

[85] I. E. Bocharova, B. D. Kudryashov, and V. Skachek, "Performance of ML decoding for ensembles of binary and nonbinary regular LDPC codes of finite lengths." in IEEE International Symposium on Information Theory (ISIT), 2017, pp. 794-798.