

Nonbinary LDPC Coding for Multicarrier Underwater Acoustic Communication

Jie Huang, Shengli Zhou, and Peter Willett

Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, 06269

Abstract—In this paper, we propose to use nonbinary low density parity check (LDPC) codes to address two main issues in underwater acoustic OFDM communication: i) plain OFDM has poor performance in the presence of channel fading, and ii) OFDM transmission has a high peak-to-average-power ratio (PAPR). We propose new methods to construct nonbinary irregular LDPC codes that achieve excellent performance, match well with the underlying modulation, and can be encoded in linear time and in parallel. Simulation and experimental results confirm the excellent performance of the proposed nonbinary LDPC codes. Based on the property that the generator matrix of LDPC codes has high density, we further show how to reduce the PAPR considerably with minimal overhead.

I. INTRODUCTION

Multicarrier underwater acoustic communication, in the form of orthogonal frequency division multiplexing (OFDM), has been actively investigated recently; see e.g., [1]–[4] and references therein. The key focus has been on how to *make OFDM work* in the presence of fast channel variations. Experimental results in [5]–[7] have demonstrated that OFDM is not only feasible but also flexible for underwater acoustic channels.

However, two other main issues must be adequately addressed to successfully deploy OFDM in a practical system:

- 1) Plain (or uncoded) OFDM has poor performance in the presence of channel fading, since it does not exploit the frequency diversity inherent in the channel.
- 2) OFDM transmission has a high peak-to-average-power ratio (PAPR). A large power backoff reduces the power efficiency and limits the transmission range.

In this paper, we propose to use nonbinary LDPC codes to address these two issues for multicarrier underwater acoustic communication.

Dedicated studies of coding for underwater acoustic communication are quite limited. An underwater communication system often picks up a well-studied coding scheme from existing literature. For example, trellis coded modulation (TCM) was used together with single carrier transmission and equalization in [8]. Convolutional codes and Reed Solomon (RS) codes have been examined in [9] for underwater acoustic communication. In conjunction with spatial multiplexing, Turbo codes were used in [10] for a single-carrier underwater system with multiple transmitters. Space time trellis codes have been tested in [10] as well. For coding in underwater

OFDM communication, serially concatenated convolutional codes have been used in [1], where only a non-iterative receiver was tested.

LDPC codes [11] are capacity-achieving codes, and have been extensively studied for wireless radio systems. Relative to binary LDPC codes, one unique advantage of nonbinary LDPC codes is that they can match very well the underlying modulation. Nonbinary LDPC codes were first combined with high order modulation in a MIMO radio communication system with two transmitters and two receivers [12]. Simulations in [13] show that an iterative receiver with nonbinary LDPC codes over GF(16) can outperform the best optimized binary LDPC code *in both performance and complexity*, while a non-iterative receiver with regular LDPC cycle code over GF(256) can achieve much better performance with comparable decoding complexity compared to the binary iterative system [13].

Due to the limited bandwidth, high order constellations are desirable for multicarrier underwater communication. As such, nonbinary LDPC code is one attractive choice to be used with underwater OFDM. Our contributions in this paper are as follows.

- 1) We propose to use nonbinary LDPC codes in multicarrier underwater acoustic communication. We develop a code design procedure that leads to nonbinary LDPC codes with superior performance, while their encoding can be done in linear time and in parallel.
- 2) We present extensive simulation results that serve as benchmarks for future multicarrier underwater modem design. Experimental results confirm the excellent performance of LDPC codes.
- 3) We show how the LDPC codes can be used for PAPR reduction, based on the property that they have high-density generator matrices.

The rest of this paper is organized as follows. We describe the system model in Section II, and present the proposed nonbinary LDPC codes in Section III. Simulation and experimental results are reported in Section IV. Using LDPC codes for PAPR reduction is presented in Section V. Conclusions are contained in Section VI.

II. SYSTEM MODEL

Fig. 1 shows the block diagram of an underwater OFDM system with nonbinary LDPC coding. Consistent with the block-by-block OFDM receiver in [5], encoding and decoding are done for each OFDM block separately.

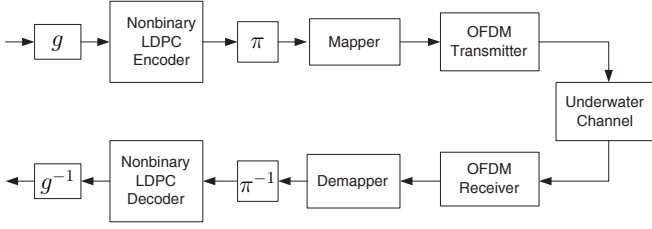


Fig. 1. A schematic block diagram of nonbinary LDPC coded OFDM system.

Suppose that an LDPC code over $\text{GF}(q)$ is used where $q = 2^p$. Let $\{\alpha_0 = 0, \alpha_1, \dots, \alpha_{q-1}\}$ denote elements in $\text{GF}(q)$. Suppose that a constellation size of $M = 2^b$ will be used by the OFDM modulator. One advantage of nonbinary LDPC coding is that one can match the field order with the constellation size, i.e., $p = b$. This way, one element in $\text{GF}(q)$ is mapped to one point in the signal constellation. In some situations when b is small, it may be preferable to choose $p > b$. Assuming that $J := p/b$ is an integer, each element in $\text{GF}(q)$ will be mapped to J symbols drawn from the constellation. Let us describe the mapper as:

$$\alpha_i \longrightarrow [\phi^0(\alpha_i), \dots, \phi^{J-1}(\alpha_i)], \quad i = 0, \dots, q-1 \quad (1)$$

where $\phi^j(\alpha_i)$ is one point in the signal constellation.

Suppose that K_d subcarriers are used for data transmission, and the LDPC code rate is r . The transmitter operates as follows. For each OFDM block, rbK_d information bits are mapped to rbK_d/p symbols in $\text{GF}(q)$, with every p bits mapped to a single $\text{GF}(q)$ symbol through a bit-to-symbol mapper g . The LDPC encoder outputs bK_d/p coded symbols in $\text{GF}(q)$, which pass through a coded-symbol interleaver π to obtain a vector

$$\mathbf{u} = [u[0], \dots, u[K_d/J - 1]]^T. \quad (2)$$

The mapper in (1) maps the vector \mathbf{u} to a modulated-symbol vector $\mathbf{s} := [s[0], \dots, s[K_d - 1]]^T$ as

$$\mathbf{s} = [\phi^0(u[0]), \dots, \phi^{J-1}(u[0]), \phi^0(u[1]), \dots, \phi^{J-1}(u[K_d/J - 1])]^T. \quad (3)$$

The K_d entries of \mathbf{s} are distributed to the OFDM data subcarriers. An OFDM transmission is formed after mixing the data subcarriers with pilot and null subcarriers [5].

Using the block-by-block OFDM receiver in [5], the equivalent channel input-output model on the data subcarriers is

$$y[k] = H[k]s[k] + n[k], \quad k = 0, \dots, K_d - 1, \quad (4)$$

where $H[k]$ is the channel frequency response on the k th data subcarrier, $y[k]$ is the output on the k th data subcarrier, and $n[k]$ is the additive noise plus the residual inter-carrier-interference. Assume that $n[k]$ has variance σ^2 per real and imaginary dimension.

The demapper computes the likelihood

$$\Pr(u[k] = \alpha_i) \propto \exp\left(\frac{-\sum_{j=0}^{J-1} |y[kJ + j] - H[kJ + j]\phi^j(\alpha_i)|^2}{2\sigma^2}\right),$$

$$k = 0, \dots, K_d/J - 1; \quad i = 0, \dots, q - 1.$$

where $|\cdot|$ denotes the absolute value of a complex number. The likelihood values are passed to the deinterleaver π^{-1} before being passed to the LDPC decoder. The FFT-based q -ary sum-product algorithm (FFT-QSPA) [14] can be used for iterative decoding. After a finite number of decoding iterations, hard decisions on the nonbinary symbols will be made at the output of the LDPC decoder, based on which information bits are found.

Unlike a system with binary coding and high order modulation, the proposed system in Fig. 1 does not require any iterative processing between the demapper and the LDPC decoder.

III. THE PROPOSED NONBINARY LDPC CODES

Let \mathbf{H} denote the parity-check matrix of an LDPC code. Suppose that the size of \mathbf{H} is $m \times n$. An $n \times 1$ vector \mathbf{x} with entries from $\text{GF}(q)$ is a valid codeword if and only if $\mathbf{H}\mathbf{x} = \mathbf{0}$. An LDPC code whose \mathbf{H} has fixed column weight and fixed row weight is called a regular code. An LDPC code whose \mathbf{H} has fixed column weight $j = 2$ is called a cycle code [15], which could be regular or irregular. In this paper, we will consider both regular and irregular LDPC codes over $\text{GF}(q)$. For regular LDPC codes, we will consider cycle codes that have fixed column weight 2 and fixed row weight d . We will then develop a novel method to construct irregular LDPC codes that have mixed column weights of 2 and t , where $t \geq 3$.

A. Nonbinary Regular Cycle Code

LDPC cycle codes over $\text{GF}(2^p)$ can achieve near-Shannon-limit performance as p increases, as shown in [15]. Further, it is shown in [16] that the column degree distribution of a good nonbinary LDPC code tends to be *ultra sparse* for large q . Therefore, the family of cycle codes are attractive when a large q is selected.

Using tools from graph theory, we have shown in [17] that the check matrix \mathbf{H} of regular cycle codes is well structured. Specifically, the parity check matrix \mathbf{H} of any regular cycle code can be put into a *concatenation form of row-permuted block-diagonal matrices* after row and column permutations if its row weight d is even, or, if d is odd and the code's associated graph [18] contains at least one spanning subgraph that consists of disjoint edges. For convenience, let us state Theorem 1 of [17] here.

Theorem 1 of [17]: *For a cycle $\text{GF}(q)$ code, if its associated graph G is d -regular with $d = 2r$, its parity check matrix \mathbf{H} of size $m \times n$ has the equivalent form*

$$\mathbf{H} \cong [\bar{\mathbf{H}}_1, \mathbf{P}_2 \bar{\mathbf{H}}_2, \dots, \mathbf{P}_r \bar{\mathbf{H}}_r], \quad (5)$$

where \mathbf{P}_i is an $m \times m$ permutation matrix, and $\bar{\mathbf{H}}_i$ is of size $m \times m$, $1 \leq i \leq r$. The matrix $\bar{\mathbf{H}}_i$ has an equivalent block-diagonal form

$$\bar{\mathbf{H}}_i \cong \text{diag}(\tilde{\mathbf{H}}_{i,1}^c, \tilde{\mathbf{H}}_{i,2}^c, \dots, \tilde{\mathbf{H}}_{i,L_i}^c), \quad (6)$$

where the matrix $\tilde{\mathbf{H}}_{i,l}^c$ is of size $k_{i,l} \times k_{i,l}$ that satisfies $m = \sum_{l=1}^{L_i} k_{i,l}$ and has an equivalent form

$$\tilde{\mathbf{H}}^c = \begin{bmatrix} \alpha_1 & 0 & 0 & \dots & \beta_k \\ \beta_1 & \alpha_2 & 0 & \dots & 0 \\ 0 & \beta_2 & \alpha_3 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \beta_{k-1} & \alpha_k \end{bmatrix} \quad (7)$$

where α_i s and β_i s are nonzero entries from $\text{GF}(q)$.

With this structure, nonbinary regular cycle codes possesses several desirable properties [17]: i) encoding can be done in linear-time and in parallel; ii) sequential belief propagation (BP) decoding can be implemented with parallel processing; and iii) the storage for the parity check matrix is reduced.

Denote the *designed code rate* of an LDPC code with \mathbf{H} of size $m \times n$ as $R = (n - m)/n$. Due to the constraint of $md = 2n$, the designed code rate of regular cycle codes is restricted to

$$R = \frac{n - m}{n} = \frac{d - 2}{d}, \quad (8)$$

where d is an integer. For example, R can be $\frac{1}{3}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \dots, \frac{7}{8}, \dots, \frac{15}{16}, \dots$.

B. Nonbinary Irregular LDPC Code

Cycle codes over large Galois fields (e.g., $q \geq 64$) can achieve near-Shannon-limit performance. However, the performance gain brought by using LDPC cycle codes over large Galois fields comes along with a significant increase of the decoding complexity. LDPC codes over moderate Galois fields (e.g., $4 \leq q \leq 32$) may be attractive from the decoding complexity point of view. We have observed a high error floor for cycle codes over $\text{GF}(q)$ with moderate q . The high error floor is mainly caused by undetected errors which are due to the codes' poor distance spectrum. In order to lower the error floor of cycle codes, here we propose a simple strategy to increase the code's performance for high SNR. We adopt irregular column weight distribution, replacing a portion of columns of weight 2 of \mathbf{H} by columns of weight $t > 2$, (e.g., $t = 3$ or $t = 4$). This strategy has three effects:

- It increases the minimum Hamming distance of the code;
- It decreases the multiplicities of low weight codewords;
- It probably improves the code performance at the waterfall region due to irregular column degree distribution.

Specifically, let \mathbf{H} have n_1 columns having weight 2 and n_2 columns having weight t . The mean column weight is

$$\eta = \frac{2n_1 + tn_2}{n} = 2 + (t - 2)\frac{n_2}{n}. \quad (9)$$

The matrix \mathbf{H} can be arranged as

$$\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H}_2], \quad (10)$$

where \mathbf{H}_1 contains all weight 2 columns and \mathbf{H}_2 contains all weight t columns. Clearly \mathbf{H}_1 is of size $m \times n_1$ and \mathbf{H}_2 is of size $m \times n_2$.

Now we need to design \mathbf{H}_1 and \mathbf{H}_2 . To maximally benefit from the structure we have developed for regular cycle code in Section II.A, we propose to use the following design rule. Note that \mathbf{H}_1 corresponds to the check matrix of a general cycle code. We would like \mathbf{H}_1 to be as close to a regular cycle code as possible. Specifically, we split the matrix as

$$\mathbf{H} = [\mathbf{H}_{1a} \mid \mathbf{H}_{1b} \mid \mathbf{H}_2], \quad (11)$$

where the matrix \mathbf{H}_{1a} is of size $m \times n_{1a}$ and the matrix \mathbf{H}_{1b} is of size $m \times n_{1b}$. The number n_{1a} is the largest integer not greater than n_1 that can render $d_{1a} = \frac{2n_{1a}}{m}$ an integer; that is, \mathbf{H}_{1a} is the largest sub-matrix of \mathbf{H}_1 that could be made d_{1a} -regular. If $n_{1a} = n_1$, then $n_{1b} = 0$. As such, \mathbf{H}_1 itself can be made regular, which is a special case.

The detailed design steps are as follows.

- **Step 1:** *Specify the structure of \mathbf{H}_{1a} .* Construct a cycle code of fixed row weight d_{1a} using the design methodologies presented in [17].
- **Step 2:** *Specify the structure of \mathbf{H}_{1b} and \mathbf{H}_2 .* Apply the progressive edge-growth (PEG) algorithm [19] to attach n_{1b} columns of weight 2 and n_2 columns of weight t to the matrix \mathbf{H}_{1a} . This way, the structure of \mathbf{H} in (11) is established.
- **Step 3:** *Specify the non-zero entries of \mathbf{H}_1 .* We can regard the submatrix $\mathbf{H}_1 = [\mathbf{H}_{1a} \mid \mathbf{H}_{1b}]$ as a check matrix of a cycle code. Hence, we can apply the design criterion of [17] to choose appropriate nonzero entries for \mathbf{H}_1 to make as many as possible short length cycles of the associated graph [18] of \mathbf{H}_1 irresolvable.
- **Step 4:** *Specify the non-zero entries of \mathbf{H}_2 .* The nonzero entries of \mathbf{H}_2 are generated randomly with a uniform distribution over the set $\text{GF}(q) \setminus 0$.

The proposed nonbinary irregular LDPC codes try to make a large portion of its check matrix into a regular cycle code. This way, many benefits from regular cycle codes can be retained.

As illustration, Fig. 2 compares the performance of irregular LDPC codes over $\text{GF}(16)$ with different mean column weights. All the codes have rate of 1/2 and block length of 1008 bits. BPSK modulation is used on the binary input AWGN channel and the decoder uses the sequential BP algorithm with a maximum of 80 iterations. We observe from Fig. 2 that the codes with $\eta = 2.0$ and $\eta = 2.2$ show an error floor above 10^{-5} which are caused by undetected errors. No error floor above 10^{-5} shows if $\eta \geq 2.4$. Actually no undetected errors have been observed for $\eta \geq 2.4$ in our simulations. Another interesting observation is that as η increases from 2.4 to 2.6 and 2.8, the code performance degrades. Therefore, the code with $\eta = 2.4$ is the best one in this setting. Fig. 3 shows the performance comparison between the irregular LDPC codes over $\text{GF}(16)$ with binary optimized LDPC code. The performance of Mackay's (3,6)-regular code

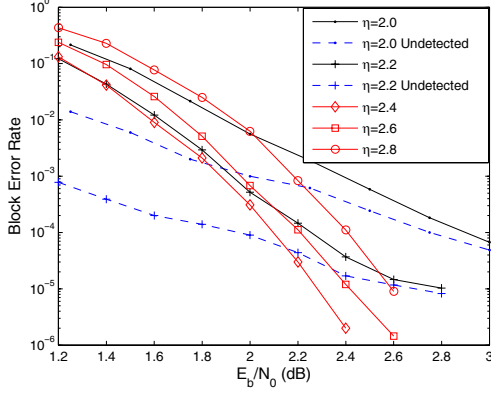


Fig. 2. Performance comparison of irregular codes over GF(16) with different mean column weights. $t = 3$, $r = 1/2$, and the block length is 1008 bits. For the $\eta = 2.0$ and $\eta = 2.2$ cases, we also plot the probability of undetected errors, which contributes to the error floor of the block error rate.

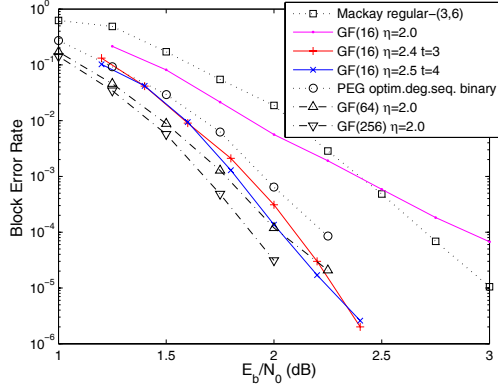


Fig. 3. Performance comparison of irregular codes over GF(16) with binary optimized irregular LDPC code. $r = 1/2$ and the block length is 1008 bits.

and cycle codes over GF(64) and GF(256) are also included [17]. It can be seen from Fig. 3 that by adopting an irregular column weight distribution, the code's performance has been greatly improved.

C. Linear-time encoding in parallel

Decoding of LDPC codes can use standard sum-product algorithms and its low-complexity variants, while encoding has been a key issue for LDPC codes. Encoding of a general LDPC code can be done in linear time instead of quadratic on the block length [20].

The constructed LDPC codes can be encoded in linear time and in parallel as follows. Assume $n_1 \geq m$, then $n_{1a} \geq m$. Since \mathbf{H}_{1a} is regular, it can be decomposed as in (5). Hence, the first $m \times m$ submatrix of \mathbf{H} can be made to have the form in (6). Let us denote it as $\tilde{\mathbf{H}}_1$, and thus we can split \mathbf{H} as $\mathbf{H} = [\tilde{\mathbf{H}}_1 \mid \mathbf{H}']$ where \mathbf{H}' is of size $m \times (n - m)$. Partition the codeword \mathbf{x} into two parts as $\mathbf{x} = [\mathbf{p}^T, \mathbf{s}^T]^T$ where \mathbf{p} is of length m . We make sure that $\tilde{\mathbf{H}}_1$ is full rank, let \mathbf{p} contains the parity symbols and \mathbf{s} contains the information symbols. A

valid codeword satisfies $\mathbf{H}\mathbf{x} = \mathbf{0}$, which implies that

$$\tilde{\mathbf{H}}_1 \mathbf{p} = -\mathbf{H}'\mathbf{s}. \quad (12)$$

From (6), $\tilde{\mathbf{H}}_1$ is block diagonal $\text{diag}(\tilde{\mathbf{H}}_{1,1}^c, \dots, \tilde{\mathbf{H}}_{1,L_1}^c)$. According to the sizes of $\{\tilde{\mathbf{H}}_{1,i}^c\}_{i=1}^{L_1}$, let us partition \mathbf{p} and the right-hand side of (12) into L_1 pieces as $[\mathbf{p}_1^T, \dots, \mathbf{p}_{L_1}^T]^T$ and $[\mathbf{b}_1^T, \dots, \mathbf{b}_{L_1}^T]^T$, respectively. The computation of \mathbf{p} requires solving the following L_1 equations

$$\tilde{\mathbf{H}}_{1,i}^c \mathbf{p}_i = \mathbf{b}_i, \quad 1 \leq i \leq L_1. \quad (13)$$

A linear time algorithm for solving these equations has been proposed in Lemma 4 of [18]. Note that solving these L_1 equations can be performed in parallel, thus encoding can be performed in linear time and *in parallel*. This provides flexibility in the implementation of efficient encoders, which is quite desirable especially when the block length is large. Note that the universal linear-time encoding algorithm of [18] for cycle codes works only in a serial manner.

IV. PERFORMANCE RESULTS

We simulate the system performance using both an AWGN channel and an underwater Rayleigh fading channel with the OFDM parameters as in [5] and [6]. Specially, the bandwidth is 12 kHz, and the channel delay spread is 10 ms, resulting in 120 channel taps in discrete-time. We use equal-variance complex Gaussian random variables on each tap. Each OFDM block is of duration 85.33 ms, and has 1024 subcarriers, out of which 672 subcarriers are used for data transmission. Each OFDM block contains one codeword. The FFT-QSPA algorithm [14] is used for nonbinary LDPC decoding, where the maximum number of iterations is set to 80. Gray labelling and random interleavers are used in all the simulations.

Matching the LDPC codes with BPSK, QPSK, 16QAM and 64QAM constellations, we have constructed 6 appropriate operation modes, as listed in Table I. The bandwidth efficiency ranges from 0.5 to 5.25 bit/s/Hz.

Test Case 1 (Performance of different modes). Fig. 4 shows the block error rate (BLER) performance of all the modes in Table I over an AWGN channel. Also included are the uncoded BER curves for different modulations. Figs. 5 and 6 show the BLER and BER performance of all the modes in Table I over OFDM Rayleigh fading channel respectively. Also included

TABLE I
NONBINARY LDPC CODES DESIGNED FOR UNDERWATER SYSTEM. η STANDS FOR MEAN COLUMN WEIGHT. EACH CODEWORD HAS 672b BITS WITH A SIZE- 2^b CONSTELLATION

Mode	Bit/s/Hz	Rate	η	t	Galois field	Constellation
1	0.5	1/2	2.8	4	GF(4)	BPSK
2	1	1/2	2.8	4	GF(4)	QPSK
3	2	1/2	2.3	3	GF(16)	16QAM
4	3	1/2	2.0	-	GF(64)	64QAM
5	4.5	3/4	2.0	-	GF(64)	64QAM
6	5.25	7/8	2.0	-	GF(64)	64QAM

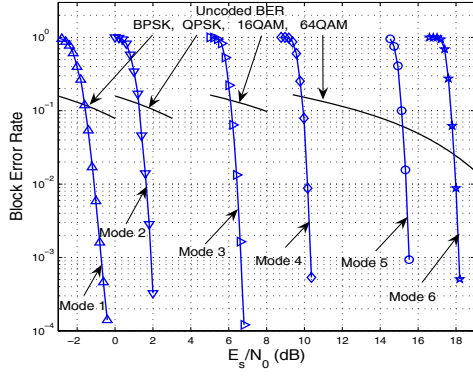


Fig. 4. BLER of different modes over AWGN channel.

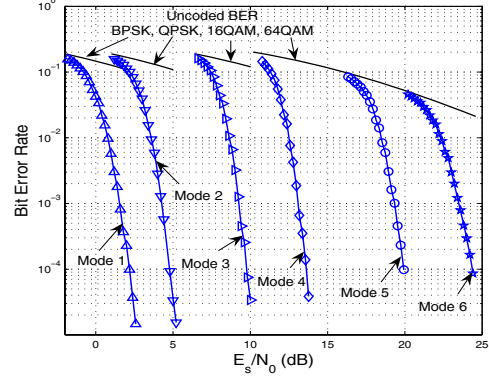


Fig. 6. BER of different modes over OFDM fading channel.

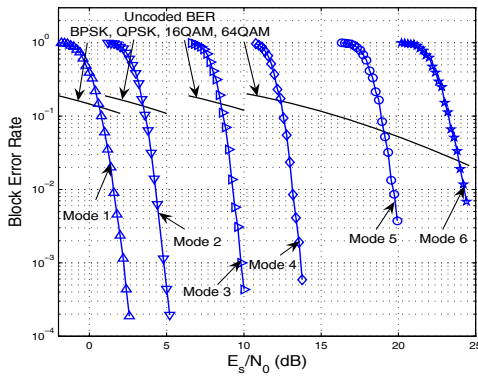


Fig. 5. BLER of different modes over OFDM fading channel.

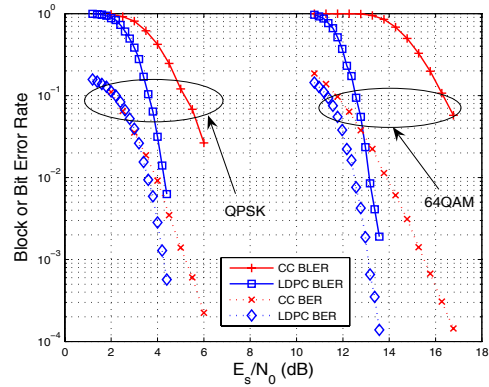


Fig. 7. Comparison between LDPC and CC codes of rate 1/2 under different modulation over OFDM Rayleigh fading channel.

are the uncoded BER curves for different modulations. We see that as long as uncoded BER is somewhat below 0.1, the coding performance improves drastically, approaching the waterfall behavior.

Test Case 2 (Comparison with CC based BICM). Fig. 7 compares the performance between a bit-interleaved coded-modulation (BICM) system based on a 64-state rate-1/2 convolutional code and the proposed nonbinary LDPC coding system under different modulation schemes over the OFDM Rayleigh fading channel. Soft-decision Viterbi decoding is used in BICM. Compared with the BICM system with the convolutional code, nonbinary LDPC codes achieve several decibels (varying from 2 to 5 dB) performance gain at BLER of 10^{-2} .

Test results with real data. We have used the proposed nonbinary LDPC codes for several underwater experiments, and the test results are published in [6], [7]. In all experimental settings with LDPC, nearly error-free performance was achieved. Whenever the uncoded BER is below 0.1, we did not observe decoding errors for rate 1/2 codes in our experiments. This is consistent with Figs. 4–6. Hence, *the goal of OFDM demodulation is to achieve an uncoded BER to be within the range of 0.1 and 0.01, and the coding will then boost the system performance.*

V. PEAK-TO-AVERAGE POWER RATIO REDUCTION

Various PAPR reduction methods have been proposed for radio OFDM systems [21]. In this paper, we focus on the selected mapping (SLM) approach in [22], [23]. In SLM, the transmitter generates a set of sufficiently different candidate signals which all represent the same information and selects the one with the lowest PAPR for transmission. In the original SLM approach [22], side information on which signal candidate has been chosen needs to be transmitted. This causes signalling overhead. In addition, side information has high importance and has to be strongly protected. In the modified approach [23], some additional bits, used to select different scrambling code patterns, are inserted to the information bits, before applying scrambling and channel encoding. This way, the side information bits are contained in the data and do not need separate encoding.

The fact that the generator matrix \mathbf{G} of a LDPC code has high density is well known [20], but rarely utilized. Here we use this property of LDPC to reduce PAPR, following the principle of SLM in [23]. The transmitter operates as follows:

- For each set of information bits to be transmitted within one OFDM symbol, reserve z bits for PAPR reduction purpose.
- For each choice of the values of these z bits, carry out

LDPC encoding and OFDM modulation, and calculate the PAPR.

- Out of 2^z candidates, select the OFDM symbol with the lowest PAPR for transmission.

Compared with [23], the proposed method bypasses the scrambling operation at the transmitter and the descrambling operation at the receiver. Due to the non-sparseness of \mathbf{G} , single bit change will lead to a drastically different codeword after LDPC encoding [20]. Since z is very small, the reduction on transmission rate is negligible. At the receiver side, those z bits are simply dropped after channel decoding. The main complexity increase is hence on the transmitter. Fast encoding as presented in Section III-C is thus very important for the proposed approach.

We now simulate the complementary cumulative distribution function (ccdf) of PAPR, $\Pr(\text{PAPR} > x)$, as a function of the number of overhead bits. The baseband PAPR ccdf curves for 'Mode 2' system in Table I by using the proposed nonbinary LDPC code and a 64-state rate-1/2 convolutional code are shown in Fig. 8 for $z = 0$, $z = 2$ and $z = 4$ respectively, where oversampling with a factor of 4 is used. The generator matrix of convolutional code has low density, as each bit can only affect subsequent bits within the constraint length. For convolutional codes, the z index bits are distributed uniformly among the information bit sequence. As shown in Fig. 8, using nonbinary LDPC code with 4 bits overhead can achieve about 3dB gain than the case with no overhead at ccdf of 10^{-3} . Compared with convolutional codes using 4 bits overhead, nonbinary LDPC code with 4 bits overhead can achieve about 2dB gain at ccdf of 10^{-3} . Hence, scrambling is not needed for LDPC codes, but necessary for convolutional codes.

For high rate codes, nonsystematic LDPC codes can have better PAPR reduction relative to systematic LDPC codes.

VI. CONCLUSION

In this paper, we proposed the use of nonbinary LDPC codes in multicarrier underwater acoustic communication. We proposed novel codes that match well with the signal constellation, have excellent performance, and can be encoded in linear time and in parallel. Extensive simulations together with a summary on field test results are presented. We also showed the use of LDPC codes to reduce the peak to average power ratio in OFDM transmissions.

REFERENCES

- [1] M. Chitre, S. H. Ong, and J. Potter, "Performance of coded OFDM in very shallow water channels and snapping shrimp noise," in *Proceedings of MTS/IEEE OCEANS*, vol. 2, 2005, pp. 996–1001.
- [2] P. J. Gendron, "Orthogonal frequency division multiplexing with on-off-keying: Noncoherent performance bounds, receiver design and experimental results," *U.S. Navy Journal of Underwater Acoustics*, vol. 56, no. 2, pp. 267–300, Apr. 2006.
- [3] M. Stojanovic, "Low complexity OFDM detector for underwater channels," in *Proc. of MTS/IEEE OCEANS conference*, Boston, MA, Sept. 18-21, 2006.
- [4] B. Li, S. Zhou, M. Stojanovic, and L. Freitag, "Pilot-tone based ZP-OFDM demodulation for an underwater acoustic channel," in *Proc. of MTS/IEEE OCEANS conference*, Boston, MA, Sept. 18-21, 2006.

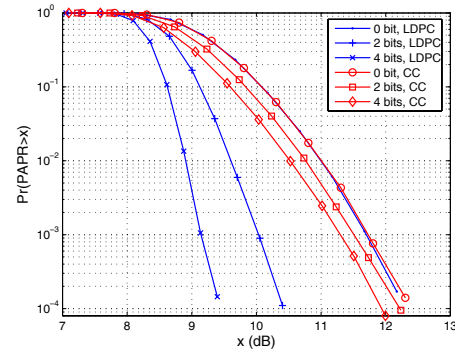


Fig. 8. Comparison of PAPR reduction using LDPC and CC code.

- [5] B. Li, S. Zhou, M. Stojanovic, L. Freitag, and P. Willett, "Non-uniform Doppler compensation for zero-padded OFDM over fast-varying underwater acoustic channels," in *Proc. of MTS/IEEE OCEANS conference*, Aberdeen, Scotland, June 18-21, 2007.
- [6] B. Li, S. Zhou, M. Stojanovic, L. Freitag, J. Huang, and P. Willett, "MIMO-OFDM over an underwater acoustic channel," in *Proc. of MTS/IEEE OCEANS conference*, Vancouver, Canada, Sept. 30-Oct. 4, 2007.
- [7] B. Li, S. Zhou, J. Huang, and P. Willett, "Scalable OFDM design for underwater acoustic communications," in *Proc. of Intl. Conf. on ASSP*, Las Vegas, NV, Mar. 3 – Apr. 4, 2008.
- [8] M. Stojanovic, J. A. Catipovic, and J. G. Proakis, "Phase-coherent digital communications for underwater acoustic channels," *IEEE Journal of Oceanic Engineering*, vol. 19, no. 1, pp. 100–111, Jan. 1994.
- [9] A. Goalic, J. Trubuil, and N. Beuzelin, "Channel coding for underwater acoustic communication system," in *Proc. of OCEANS*, Boston, MA, Sept. 18-21, 2006.
- [10] S. Roy, T. M. Duman, V. McDonald, and J. G. Proakis, "High rate communication for underwater acoustic channels using multiple transmitters and space-time coding: Receiver structures and experimental results," *IEEE Journal of Oceanic Engineering*, 2008 (to appear).
- [11] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.
- [12] F. Guo and L. Hanzo, "Low complexity non-binary LDPC and modulation schemes communicating over MIMO channels," in *Proc. of VTC*, vol. 2, pp. 1294–1298, Sept. 26-29, 2004.
- [13] R.-H. Peng and R.-R. Chen, "Design of nonbinary LDPC codes over GF(q) for multiple-antenna transmission," in *Proc. of Military Communications conference 2006*, Washington, DC, Oct. 23-25 2006, pp. 1–7.
- [14] H. Song and J. R. Cruz, "Reduced-complexity decoding of q-ary LDPC codes for magnetic recording," *IEEE Trans. Magn.*, vol. 39, pp. 1081–1087, 2003.
- [15] X.-Y. Hu and E. Eleftheriou, "Binary representation of cycle tanner-graph GF(2^b) codes," *Proc. of International Conference on Communications*, vol. 27, no. 1, pp. 528 – 532, June 2004.
- [16] M. C. Davey, *Error-Correction using Low-Density Parity-Check Codes*. Dissertation, University of Cambridge, 1999.
- [17] J. Huang, S. Zhou, and P. Willett, "On regular LDPC cycle codes over GF(q)," *IEEE Transactions on Information Theory*, submitted Oct. 2007.
- [18] J. Huang and J.-K. Zhu, "Linear time encoding of cycle GF(2^p) codes through graph analysis," *IEEE Communications Letters*, vol. 10, pp. 369–371, May 2006.
- [19] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, 2005.
- [20] D. Mackay, *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003.
- [21] S. Litsyn, *Peak Power Control in Multicarrier Communications*. Cambridge University Press, 2007.
- [22] R. Bauml, R. Fischer, and J. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping," *Electron. Lett.*, vol. 32, no. 22, pp. 2056–2057, Oct. 1996.
- [23] M. Breiling, S. Muller-Weinfurter, and J.-B. Huber, "SLM peak-power reduction without explicit side information," *IEEE Commun. Lett.*, vol. 5, no. 6, pp. 239–241, June 2001.