Nonbinary LDPC Code for Noncoherent Underwater Acoustic Communication and Its Experiment Results

Yanbo Wu, Min Zhu, Weiqing Zhu, Zeping Xing, Lijun Xu and Bo Yang
Laboratory of Ocean Acoustic Technology
Institute of Acoustic, Chinese Academy of Sciences
Beijing, China 100190
{wuyanbo,zhumin}@mail.ioa.ac.cn

***Abstract*—Noncoherent underwater acoustic communication channel in adverse condition is modeled as phase-random Rayleigh fading channel. Concatenated code based on nonbinary LDPC code and constant weight code is proposed in noncoherent communication and iteratively decoded in probability domain. Without information of channel amplitude or phase, statistic parameters of signal and noise bins were estimated based on moment estimation method, posterior probabilities of constant weight code-words were further calculated, and nonbinary LDPC code was decoded with nonbinary sum-product algorithm. It is verified by simulation that the proposed concatenated code has a 3 dB SNR benefit than non-iterative concatenated code. Underwater communication experiments were carried out in both deep ocean (vertical communication, 5 km) and shallow lake (horizontal communication, near 3 km, delay spread larger than 50 ms), signal frequency band was 6~10 kHz, and data transmission rate was 357 bps. It is shown that the proposed scheme can correctly transmit in both experiments with a signal noise ratio of 2 dB. The performance of proposed algorithm was verified by experiment.**

Keywords—Noncoherent underwater acoustic communication; Rayleigh fading channel; nonbinary LDPC code; Hadamard code

I. INTRODUCTION

Underwater acoustic channel has the characteristics of rapid variation and serious multipath, and accurate estimation of its phase is difficult in adverse condition. Therefore noncoherent communication, without need of channel phase tracking, is widely used in application of underwater acoustic communication [1-3]. The key problem of underwater acoustic communication, especially with noncoherent communication, is power consumption. Advance channel codes can decrease power consumption in transmission and improve communication reliability. However, there are seldom research reports in noncoherent underwater acoustic communication in recent years.

The noncoherent communication channel is modeled as random phase Rayleigh fading channel [3-6], and efficient anti-fading method is coding in frequency domain [5]. Constant-weight codes, for example Hadamard codes, with on-off keying modulation can provide diversity gain and are useful in noncoherent communication. The use of constant-weight codes and concatenated codes is a classic technique for noncoherent underwater acoustic communication. The concatenated code with proper parameters is concatenation of Hadamard code $H(20,5)$ and dual–k (k=5) code[3,5-8], with channel spectral efficiency is 0.125 bit / s /Hz and the minimum code distance 40. Square law combination and Viterbi decoding algorithm are used in its receiving detection. This scheme has been cited in several papers concluding noncoherent underwater acoustic communication since several decades ago. Shannon limited approaching channel codes, for example Turbo code and LDPC code [9], with iteratively decoding, have not been used in noncoherent underwater acoustic communication as we known. The problem of iteratively decoding in noncoherent channel is posterior probability calculation when both channel fading amplitude and phase are unknown.

The concatenated code of nonbinary LDPC code and Hadamard code is proposed, whose decoding processing is realized in nonbinary probability domain. The decoding is divided in 3 steps. Firstly, the amplitude statistics of the signal or noise frequency bins are estimated based on moment estimation method. Secondly, posterior probabilities of Hadamard code-words in fading channel are calculated using the amplitude statistics estimation. Thirdly, nonbinary LDPC code is iteratively decoded based on factor graph algorithm using posterior probabilities of Hadamard code-words as its input. It is verified by simulation that the proposed concatenated code has a 3 dB SNR benefit than non-iterative concatenated code. Underwater communication experiments were carried out in both deep ocean (vertical communication, 5 km) and shallow lake (horizontal communication, near 3 km, delay spread larger than 50 ms), signal frequency band was 6~10 kHz, and data transmission rate was 357 bps. It is shown that the proposed scheme can correctly transmit in both experiments with a signal noise ratio of 2 dB. The performance of proposed algorithm was verified by experiments.

II. NONCOHERENT COMMUNICATION SCHEME BASED ON NONBINARY LDPC CODE

The system diagram of noncoherent communication scheme based on nonbinary LDPC code is shown Fig. 1. Firstly, the information bit sequence is encoded in nonbinary LDPC and Hadamard code, then it is modulated with on-off keying. The multicarrier technique is adopted based on IFFT transform (IFFT: inverse fast Fourier transform), and guard interval is added to combat the multipath effect. In the receiving subsystem, synchronized waveform is matched with all in-band frequency bins by FFT transform, and modular square is calculated with these bins. With the result of

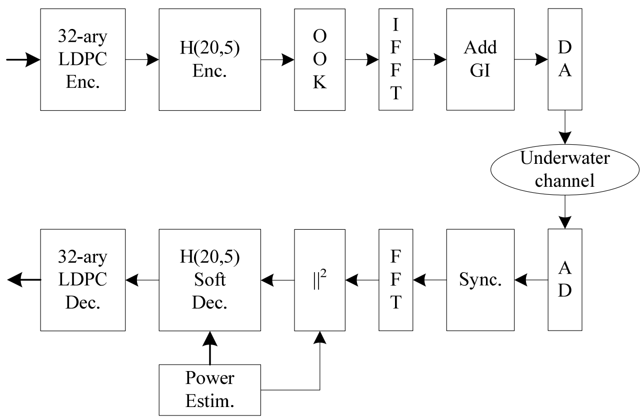

Fig. 1. Noncoherent communication based on Nonbinary LDPC code

signal and noise power estimation, posterior probabilities of Hadamard code-words are calculated and fed into the nonbinary LDPC decoder. The mainly problem to be solved is calculation of posterior probabilities of Hadamard code-words without channel status information.

A. Posterior Probabilities of Constant-weight Code-words

The posterior probabilities of Hadamard code-words are calculated with on-off keying modulation in random phase Rayleigh fading channel. The proposed method can be extended to other constant-weight code, for example Golay code. Matrix containing all Hadamard code-words is marked as

$$\mathbf{H}=\begin{bmatrix}\mathbf{c}^{(1)}\\ \mathbf{c}^{(2)}\\ \vdots\\ \mathbf{c}^{(2^k)}\end{bmatrix}=\begin{bmatrix}c_1^{(1)} & c_2^{(1)} & \cdots & c_n^{(1)}\\ c_1^{(2)} & c_2^{(2)} & \cdots & c_n^{(2)}\\ \vdots & & & \\ c_n^{(2^k)} & c_n^{(2^k)} & \cdots & c_n^{(2^k)}\end{bmatrix} \tag{1}$$

where n is length of each code-word, k is the number of input bits. For Hadamard (20, 5), that is n=20, k=5. The code-word (a row in the matrix) is selected according to the k input bits, which accomplishes encoding processing. In the random phase Rayleigh fading channel model, channel phase value is uniform distributed and memory-less, and therefore phase of received waveform carries no information. The modular squares of frequency bins carry all the information of received waveform. Supposed that received modular squares of n frequency bins are marked as $[U_1\ U_2 \dots U_n]$, E_c is energy per carrier, and N_0 is noise power spectrum density. According to Rayleigh fading distribution, received modular square distributions when transmitting 0 and 1 with on-off keying modulation are as follows:

$$\begin{cases} p\left(U\middle|s=0\right)=N_0\exp\left(-\dfrac{U}{N_0}\right)\\ p\left(U\middle|s=1\right)=\left(E_c+N_0\right)\exp\left(-\dfrac{U}{E_c+N_0}\right)\end{cases} \tag{2}$$

The posterior probability that Hadamard code $\mathbf{c}^{(j)}$ is transmitted, is calculated as conditional probability

$$\begin{aligned} & p\left(s=\mathbf{c}^{(j)}\,|\left[U_1\quad U_2\quad\cdots\quad U_n\right]\right)\\ &=\frac{p\left(s=\mathbf{c}^{(j)}\right)}{p\left(\left[U_1\quad U_2\quad\cdots\quad U_n\right]\right)}\prod_{i=1}^{n}p\left(U_i\,|\,s_i=c_i^{(j)}\right)\\ &=A_1\bullet\prod_{i=1}^{n}p\left(U_i\,|\,0\right)^{1-c_i^{(j)}}\;p\left(U_i\,|\,1\right)^{c_i^{(j)}}\\ &=A_1\bullet A_2\bullet\prod_{i=1}^{n}\left[\frac{p\left(U_i\,|\,1\right)}{p\left(U_i\,|\,0\right)}\right]^{c_i^{(j)}}\\ &=A_1\bullet A_2\bullet\exp\left\{\sum_{i=1}^{n}c_i^{(j)}\log\left[\frac{p\left(U_i\,|\,1\right)}{p\left(U_i\,|\,0\right)}\right]\right\}\\ &=A_1\bullet A_2\bullet A_3\bullet\exp\left\{\frac{E_c}{N_0\left(N_0+E_c\right)}\sum_{i=1}^{n}U_i c_i^{(j)}\right\}\end{aligned} \tag{3}$$

where $A_1=\dfrac{1}{2^k}\bullet\dfrac{1}{p\left(\left[U_1\quad U_2\quad\cdots\quad U_n\right]\right)}$, $A_2=\prod_{i=1}^{n}p\left(U_i\,|\,0\right)$, $A_3=\exp\left\{\dfrac{n}{2}\log\left[\dfrac{E_c}{N_0\left(N_0+E_c\right)}\right]\right\}$, are variables unrelated with j, and the calculation of $A_1\bullet A_2\bullet A_3$, can be executed using the relationship that

$$\sum_{j=1}^{2^k}p\left(s=\mathbf{c}^{(j)}\,|\left[U_1\quad U_2\quad\cdots\quad U_n\right]\right)=1 \tag{4}$$

(3) and (4) give the solution of Hadamard code-words detection probabilities without channel status information. In practical application, the variables E_c and N_0 are unknown and need to be estimated.

B. Signal and Noise Power Estimation

The power estimation is based on first two order moments of modular square distribution. According to (2), the probability density function of modular square random variable U can be calculated as

$$p\left(U\right)=\frac{1}{2}\left[p\left(U\middle|0\right)+p\left(U\middle|1\right)\right] \tag{5}$$

The first two moments are

$$\begin{cases} E\left(U\right)=\dfrac{N_0}{2}+\dfrac{N_0+E_c}{2}\\ E\left(U^2\right)=\left(N_0\right)^2+\left(N_0+E_c\right)^2\end{cases} \tag{6}$$

E_c and N_0 can be solved as functions of the moments

$$\begin{cases} E_c=\sqrt{2E\left(U^2\right)-4E^2\left(U\right)}\\ N_0=E\left(U\right)-\dfrac{1}{2}\sqrt{2E\left(U^2\right)-4E^2\left(U\right)}\end{cases} \tag{7}$$

In one communication packet, the received OOK modular squares are u_i ($1\le i\le M$), then the moment estimations are

$$\begin{cases} m_1 = \dfrac{1}{M}\sum_{i=0}^{M-1} u_i \\ m_2 = \dfrac{1}{M}\sum_{i=0}^{M-1} u_i^2 \end{cases} \tag{8}$$

There estimations of E_c and N_0 can be calculated as

$$\begin{cases} \hat{E}_c = \sqrt{2m_2 - 4m_1^2} \\ \hat{N}_0 = m_1 - \dfrac{1}{2}\sqrt{2m_2 - 4m_1^2} \end{cases} \tag{9}$$

In simulation, the estimation errors are less than 0.2 dB when M=620, which satisfy the request of Hadamard code-word probability estimation.

C. Nonbinary LDPC Code

LDCP code can approach channel capacity limitation in AWGN channel (AWGN: additive white Gaussian noise) [5]. The main research of LDPC code is concentrated on AWGN channel or fading channel with channel status known at receiver. Nonbinary LDPC code, which we use in noncoherent channel as outer code, is decoded based on sum product algorithm after Hadamard decoding by (3).

Channel utilization rate, diversity gain and decoding computation complexity are taken into consideration of LDPC order selection, and 32-ary quasi-cyclic LDPC code is selected as outer code, which is constructed based on finite fields, and whose input and output lengths are 310 and 620 [10-11]. α-multiplied circulant permutation matrix $H^{(1)}_{2^5,\mathrm{disp}}$ over GF(2^5) is constructed using Reed-Solomon code RS(31, 2, 30), then it is processed by array dispersion to form matrix $H^{(1)}_{2^5,2-\mathrm{f,disp},2}(10,20)$ [10]with dimension of 310*620, whose column and row weights are 3 and 6 respectively. $H^{(1)}_{2^5,2-\mathrm{f,disp},2}(10,20)$ is used as 32-ary LDPC check matrix. LDPC generation matrix G, with dimension of 620*310, is obtained by Gaussian elimination from $H^{(1)}_{2^5,2-\mathrm{f,disp},2}(10,20)$.

Input bit vector with length 1550 is represented as GF(2^5) vector x with dimension 310*1, and encoded vector is represented as GF(2^5) vector y with dimension 620*1. Then encoding process is the matrix calculation

$$y = G \bullet x \tag{10}$$

Nonbinary LDPC decoding based on factor graph is shown in Fig. 2 [12-13]. The function of permutation nodes is to realize the multiplication of variable nodes and non-zero check nodes. Walsh-Hadamard FFT and multiplication in frequency domain is fast algorithm to calculate nonbinary probability [14]. In the receiving end of communication system, nonbinary LDPC decoder is fed with decoding output of Hadamard code. LDPC iterative decoding is ended when the maximum times is reached or cyclic redundancy check is satisfied.

In computation of a decoding iteration, there are 357102 multiplications and 3720 calculations of 32-point Walsh-Hadamard FFT, one of which can be realized with 160

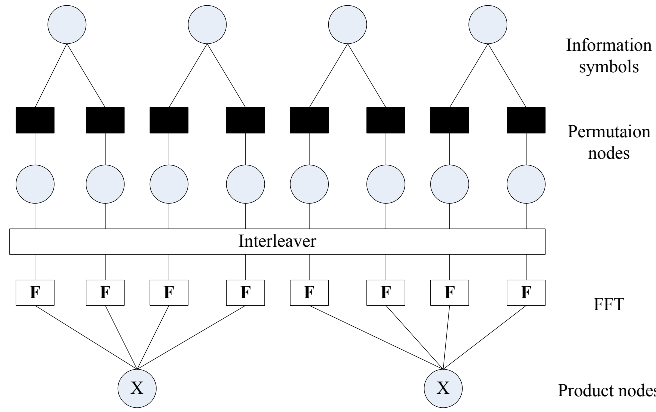

Fig. 2. Nonbinary LDPC decoding based on factor graph

additions. Supposed that the data rate of noncoherent underwater acoustic communication system is 1 kbps, and decoding is iteratively repeated to 20 times, real-time operation includes 7.7 million additions and 4.6 million multiplications per second. The computation complexity is not hard to current low power digital signal processers.

III. SIMULATION AND EXPERIMENT RESULTS

The channel model is random phase Rayleigh fading, and its amplitude and phase are unknown in receiving end. Performance of proposed concatenated code in simulation is shown in Fig. 3. The results are with different simulation conditions: maximum iterative time is 50 or 5, and average powers of signal and noise are known or unknown in receiving end. It is shown with known or estimated average powers, results are nearly the same, which verified the proposed power estimation method. The result with a maximum iterative time of 5, has 1 dB SNR loss than that of 50. The BER performance comparison among different concatenated codes based on inner code H(20,5) is shown in Fig. 4. Proposed concatenated code can make reliable transmission of E_b/N_0 = 9.3 dB (SNR = 0.3 dB) with a BER less than 0.00001, which is a 3 dB SNR improvement than concatenation of Hadamard code and dual-k code. Error correction abilities of different outer codes are shown in Fig. 5, in which horizontal axis is marked as BER of inner code's decoding result and vertical axis is marked as BER of outer code's decoding result. It is concluded that after nonbinary LDPC decoding, transmission is still reliable even if inner code's decoding (Hadamard code) has a BER of 0.2.

To verify the performance in acoustic channel, noncoherent communication experiments in both deep ocean vertical channel and shallow water horizontal channel were carried out. The frequency band was 6 to 10 kHz, 120 frequency bins with an interval of 31.25Hz were transmitted simultaneously, guard interval length was 10 ms, and information rate was 357 bps.

In the year 2011, Chinese human occupied submersible was dived into 5000 m depth in Pacific Ocean [3]. Noncoherent communication waveforms were sampled by communication device at the mother ship when the distance of submersible and ship was 5 km, and their horizontal distance was 1 km. The signal noise ratio of sampled waves exceeded 10 dB. The sample waveforms were added by noise waveforms with different SNR, and then processed using the proposed algorithm. The results are shown in table I. The concatenated code can be correctly decoded with an SNR of 2 dB. The nonbinary LDPC code can correct with an inner coder BER of 0.22, which verifies the previous simulation.

In April 2013, noncoherent communication experiment was carried out in Qiandao Lake, China. The lake depth is about 56 m depth with an unsmooth bottom. The transmitter / receiver transducers were in a depth of 15 m. The sound speed profile is shown in Fig. 6 with a relative sound speed gradient of 0.0004 / m above 25 m depth. The channel impulse response is shown in Fig. 7, and delay spread exceeds 50 ms. The performance are shown in Table II. The result of SNR requirement and error correction ability is nearly the same as in deep ocean. The iterative times are larger than that in deep ocean.

ACKNOWLEDGMENT

This work was supported by Chinese National 863 projects 2002AA401004, 2009AA093301 and 2009AA093601.

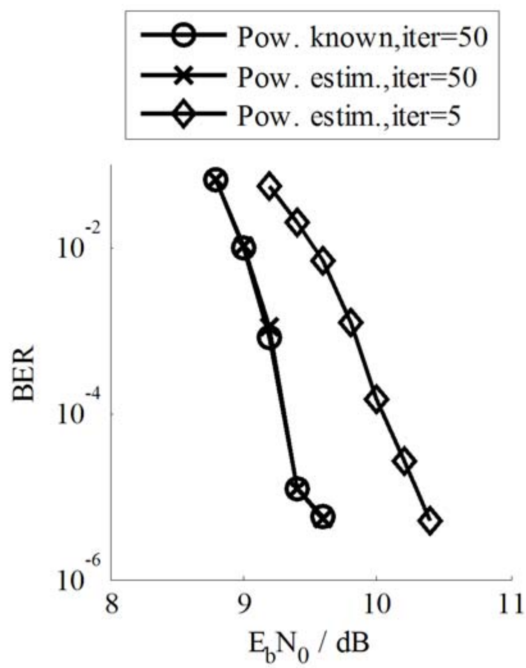

Fig. 3. BER performance of proposed concatenated code

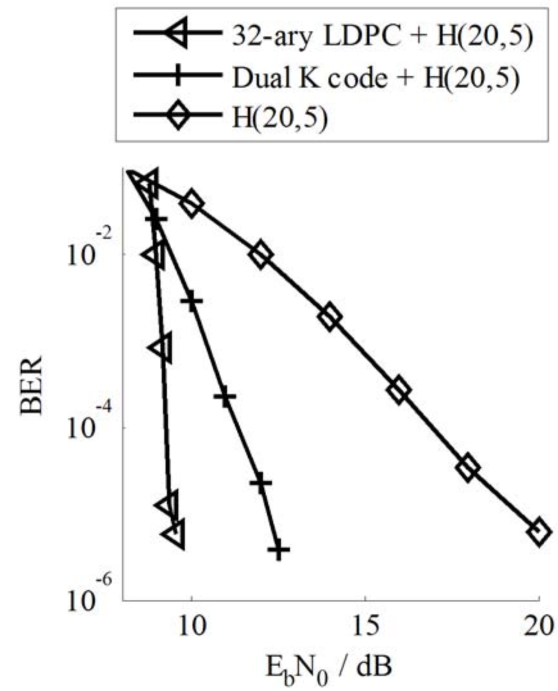

Fig. 4. BER performance comparisons among different concatenated codes

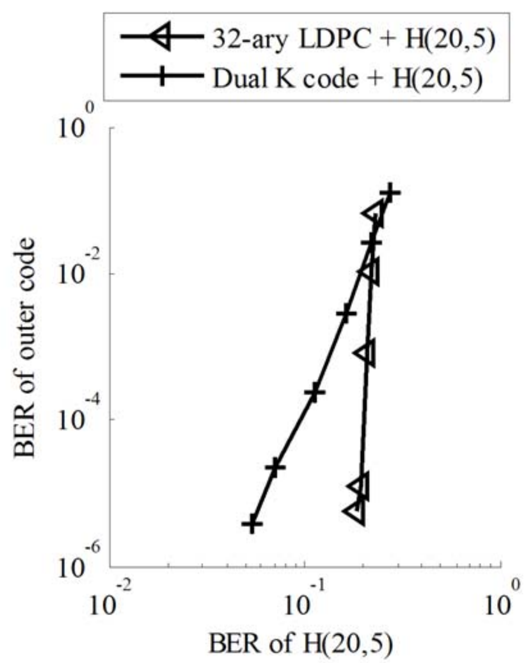

Fig. 5. Error correction abilities of different outer codes

TABLE I. BER OF CONCATENATED CODE IN 2011 DEEP OCEAN EXPERIMENT

SNR / dB	BER of Hadamard (inner code)	LDPC iterations	BER of LDPC (outer code)
0	0.28	50	0.29
1	0.25	50	0.22
2	0.20	6	0
3	0.14	4	0
4	0.12	2	0

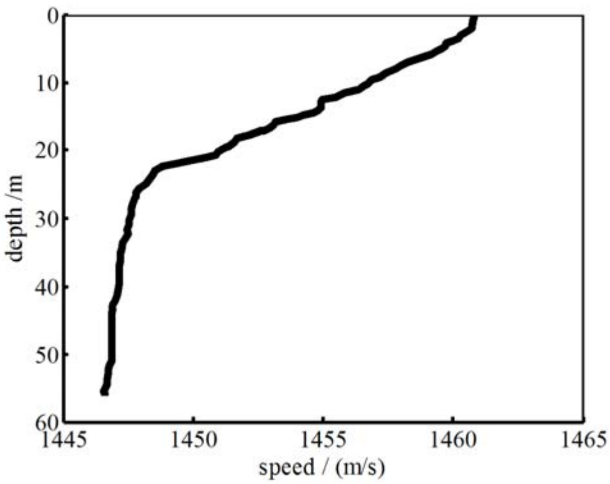

Fig. 6. Sound speed profile of Qiandao Lake in April 2013

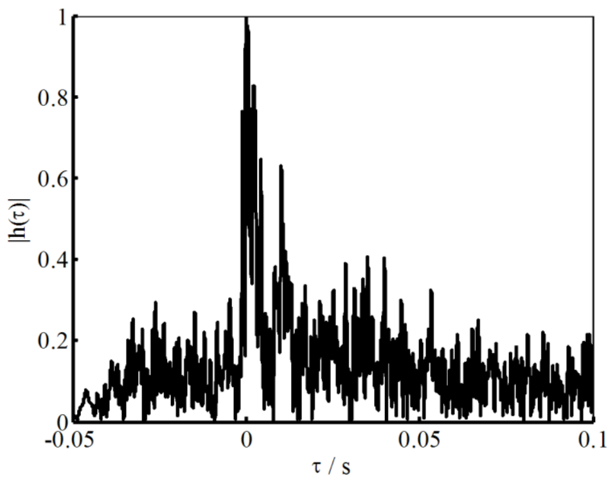

Fig. 7. Channel impulse response in 2013 Qiandao Lake experiment

TABLE II. BER OF CONCATENATED CODE IN 2013 QIANDAO LAKE EXPERIMENT

SNR / dB	BER of Hadamard (inner code)	LDPC iterations	BER of LDPC (outer code)
0	0.27	50	0.30
1	0.24	50	0.28
2	0.21	15	0
3	0.20	6	0
4	0.16	5	0

REFERENCES

[1] Green M D. Acoustic modems, navigation aids, and networks for undersea operations. OCEANS'2010 Proceedings, Sydney, 2010: 1—6

[2] Zhu Weiqing, Zhu Min, Wu Yanbo and et al. Signal processing in underwater acoustic communication system for manned deep submersible "Jiaolong". Chinese Journal of Acoustics, 2013; 32(1): 1—15

[3] Catipovic J A. Performance limitations in underwater acoustic telemetry. IEEE Journal of Oceanic Engineering, 1990; 15(3): 205—216

[4] Yang W B, Yang T C. High-frequency channel characterization for M-ary frequency shift-keying underwater acoustic communications. Journal of the Acoustical Society of America, 2006; 120(5): 2615—2626

[5] Proakis J G. Digital communications, 5 ed. New York: McGraw-Hill, 2007: 571—583

[6] Proakis J G. Coded modulation for digital communications over Rayleigh fading channels. IEEE Journal of Oceanic Engineering, 1991; 16(1): 66—73

[7] Green M D, Rice J A. Channel-tolerant FH-MFSK acoustic signaling for undersea communications and networks. IEEE Journal of Oceanic Engineering, 2000; 25(1): 28—39

[8] Kilfoyle D B, Baggeroer A B. The state of the art in underwater acoustic telemetry. IEEE Journal of Oceanic Engineering, 2000; 25(1): 4—27

[9] Singer A C, Nelson J K, Kozat S S. Signal Processing for Underwater Acoustic Communications. IEEE Communications Magazine, 2009; 47(1): 90—96

[10] Zhou Bo, Kang J Y, Song S M, Lin S, Abdel-Ghaffar K, Xu M N. Construction of non-binary quasi-cyclic LDPC codes by arrays and array dispersions. IEEE Transactions on Communications, 2009; 57(6): 1652—1662

[11] Lin S, Masse M R, Pursley M B, Royster T C, Song S. Frequency-Hop Antijam Communications with Nonbinary Error-Control Coding. Military Communications Conference Proceedings, 2007, MILCOM2007: 1—7

[12] Ryan W E, Lin S. Channel codes - classical and modern: Cambridge University Press, 2009: 484—522

[13] Kschischang F R, Frey B J, Loeliger H A. Factor graphs and the sum-product algorithm. IEEE Transactions on Information Theory, 2001; 47(2): 498—519

[14] Richardson T J, Urbanke R L. The capacity of low-density parity-check codes under message-passing decoding. IEEE Transactions Information Theory, 2001; vol. 47(2): 599—618