Low Complexity High Performance Non-Binary QC-LDPC Decoding System

Sun shulong
ssl2012@mail.ustc.edu.cn
Shanghai Institute of Microsystem and Information Technology，Chinese Academy of Sciences，Shanghai 200050，China

Lin min
Shanghai Institute of Microsystem and Information Technology，Chinese Academy of Sciences，Shanghai 200050，China

***Abstract*—Non-binary LDPC code can achieve better error correcting performance than its binary counterpart especially when the code length is short or moderate. A novel Non-Binary LDPC code is presented in this paper to replace the traditional binary standard in 802.11n system. The proposed Parity Check Matrix (PCM) is optimized by eliminating short-girths and low weight code-words. Partially-parallel quasi-cyclic structure is adopted for the encoder and the check matrix is quasi diagonal line structure. Encoding process directly utilizes check matrix rather than generator matrix to generate check sequence. For decoding process, the (Forward Backward Extended Minimum Sum (FB-EMS) algorithm is adopted. The performance of the proposed Non-binary LDPC code over GF(16) shows more than 1dB coding gain at 10^(-6) BER compared to the traditional binary standard with same bit length for 802.11n standard. Encoder structure and decoder algorithm have been also presented. For practical purposes, this Non-binary quasi-cyclic LDPC code with low complexity makes our proposed system very attractive.**

Keywords—Quasi-cyclic, Forward Backward Extended Minimum Sum (FB-EMS), Non-binary LDPC

I. INTRODUCTION

Low Density Parity Check (LDPC) code was introduced by R.G. Gallager in 1963[1] and rediscovered by MacKay in 1996 [2] [3]. The irregular LDPC code is by now the nearest code to Shannon limit with excellent error correcting performance [7].As for practical application, quasi-cyclic structure is widely used [4][8]. By extending the order from binary to Galois Filed, there exists a class of code known as non-binary LDPC code [6][11]. Non-binary LDPC code outperforms its binary counterpart in terms of decoding performance especially for short or moderate code length [9]. In current 802.11n product, binary LDPC code has been adopted as one candidate for channel coding. But for high order modulation, this architecture has to firstly translate binary sequences into symbols over GF(q), which will increase computation complexity but poorer performance. When non-binary LDPC code adopted in this system, coding and modulation can be combined jointly resulting in better error correcting performance. But the bottleneck for non-binary LDPC code application is the computation complexity for encoder and decoder. As for encoder, generator matrix is almost not sparse [12] [13], if it is calculated directly from its sparse check matrix. If the encoding process is based on generator matrix [14] [15], computation complexity will be rather huge. The encoder in this paper is based on check matrix. The check matrix is a kind of quasi-cyclic structure [18][19], so the encoder can be complemented only with right-shift units resulting in much less complexity [16][17]. As for decoding process, sum product algorithm (SPA) achieves better decoding performance[5]. To reduce complexity for implementation, various methods have been discussed, for example FFT based SPA is proposed in [10], but its complexity is still not acceptable. Forward Backward Extended Minimum Sum (FB-EMS) algorithm is adopted in this paper as its complexity can be largely reduced with little performance degradation [19] [20].

Organization of this paper is as follows: Section I introduces non-binary LDPC code related conceptions. Section II proposes the traditional binary LDPC code for 802.11n system as well as our proposed non-binary LDPC code structure. Section III contains the low complexity fast encoding process. Section IV contains Symbol Modulation and Demodulation model. Section V explains the FB-EMS decoding algorithm for non-binary LDPC code. Section VI compares and analyses the results of proposed non-binary LDPC code with traditional standard. Section VII draws conclusion of this paper.

II. PROPOSED AND TRADITIONAL QC_LDPC CODE

A binary or non-binary LDPC code is a class of linear block code defined by a sparse parity-check matrix H, where $C*H^T=0$ is the constraint condition that a valid codeword has to match, H consists of $[M_b,N_b]$ square sub-matrices and N_b equals to M_b ,the number of submatrices in horizontal direction and equals to the number of sub-matrices in vehicle direction. Each sub-matrix is either a ZxZ zero matrix or a rightly shifted identity matrix, and Z is the expansion factor and it matches the equation o $Z=N/N_b$, N equals to code length. As for 802.11n system, the code length can be 648, 1296, 1944 and code rate can be 1/2, 2/3, 3/4, 5/6, respectively. In this paper, we adopt code length 648 and code rate 1/2 to represent. The traditional binary LDPC code parity check matrix for 802.11n (648, 324) is shown in Fig.1. Parity check matrix for quasi-cyclic codes consists of several sparse rightly shifted identity matrices.

Fig.1(b) depicts a sub-matrix shifted 1 symbol from the identity matrix 27x27. Each empty square is filled with number zero and the black square is filled with number one. A square block indicates a 27x27 identity matrices, those within number is a square matrix having its rows rightly shifted. The number depicted in the square represents how many symbols the 27x27 identity matrix will rightly shift.

Fig. 2 presents our proposed novel non-binary LDPC code over GF (16) for current 802.11n standard. Its matrix consists of elements from the set $\partial \in [0, 1, \ldots, 15]$. In order to eliminate low weight codeword which is a factor for

error correcting performance we introduce the maximum prime numbers in the set α (13, 11, 7) in the matrix. As a result, our proposed structure eliminates low weight code-words and has low complexity with better performance. Each submatrix is a rightly shifted identity matrix multiplied by the number depicted in the submatrix. For LDPC code matrix, the existence of short-girths will degrade the decoding performance. As shown in Fig. 3, all the elements except for the main diagonal line is not bigger than magnitude one which means that the LDPC code has eliminated all short-girths. For proposed non-binary structure, the dimension of the matrix is 81x162 with each symbol representing 4bits. The quasi-cyclic LDPC code has also eliminated short-girths that degrade the decoding performance. This principle is firstly applied to binary LDPC code but it is more suitable for non-binary LDPC one. So for proposed non-binary LDPC structure, the decoding performance is largely increased.

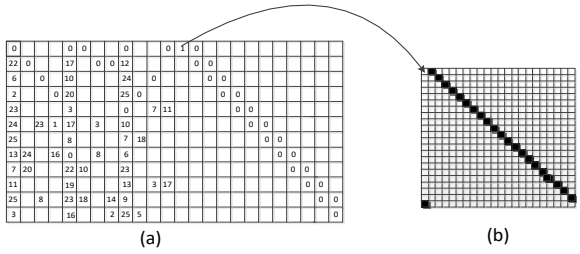


Fig. 1 (a) Binary LDPC code matrix (648,324); (b) Rightly shifted identity submatrix for 1 symbol

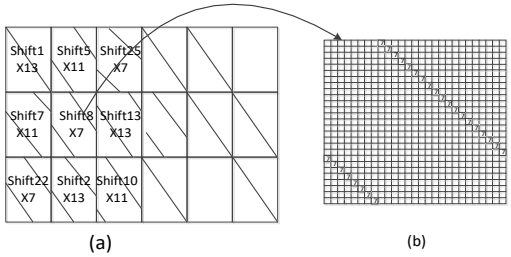


Fig .2 (a) Non-binary LDPC code over GF (16) matrix (162, 81); (b) Rightly shifted identity submatrix for 8 symbol multiplied by 7

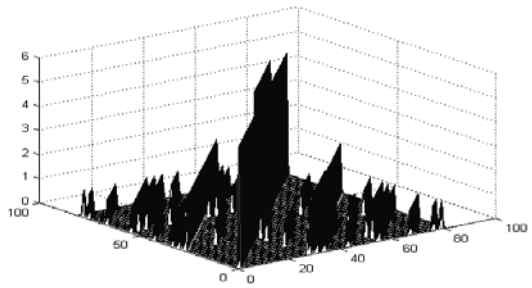


Fig .3 Short-girth Detection principle

III. LOW COMPLEXITY FAST ENCODING PROCESS

Without loss of generality, according to Equation (1), the check matrix can be divided into H1 and H2, that means H=[H1, H2], the submatrix Ix is based on the rightly shifted matrix from standard identity matrix, x indicates the bit each submatrix shifted. The dimension of the proposed structure is MxN Then H can be written as follows:

$$H = \begin{bmatrix} I_1 & I_a & \cdots & I_{a^{k-1}} & I_{x_1} & I & 0 & 0 & 0 \\ I_b & I_{a*b} & \cdots & I_{a^{k-1}*b} & 0 & I & I & 0 & 0 \\ I_{b^2} & I_{a*b^2} & \cdots & I_{a^{k-1}*b^2} & I_{x_2} & 0 & I & I & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & I & I \\ I_{b^{k-1}} & I_{a*b^{k-1}} & \cdots & I_{a^{k-1}*b^{k-1}} & I_{x_3} & 0 & 0 & 0 & I \end{bmatrix} \quad (1)$$

In order to achieve fast encoding process, the input source sequences from channel are firstly divided into blocks $S = [s0, s1, \ldots, s_{k-1}]$.The encoded data consists of source section and check section [*C, V*] ,where *V* is the check bits, the whole check sections are calculated from source bits, hence, the computation complexity for the encoder is linear to code length which makes LDPC code application attractive. All related computations are based on Galois Filed. Table 1 presents the computation complexity for proposed structure. This proposed structure has advantages in sparse matrix and reduced complexity in encoding.

Table 1 complexity of the encoder

	Multiply Complexity	Addition Complexity
V1	R(1-R)*n*n/Z	(R-1/nb)[(1-R)*nb-1]*n
V2	Rn+Z	Rn
Vi,i=3,4,5...mb	Rn	Rn
Vr+1	Rn+Z	Rn+1

Data symbols, the length of which are k*z to be encoded, are divided into k blocks firstly with each block z symbols. Then due to the structure of quasi-cycle LDPC code, the check sections can be calculated, the length of which is m*k. After encoding process, the whole entity size is *n*k.*

Just XOR gate, shift and multiplication units are involved in the encoder. So the whole encoder for implementation is largely simplified. As for this encoder, pipelined structure has been applied. As a result, the throughput is greatly improved. Fig. 4 shows the process to generate check sections. The encoder structure can be used for different applications just by slightly changing its submatrix.

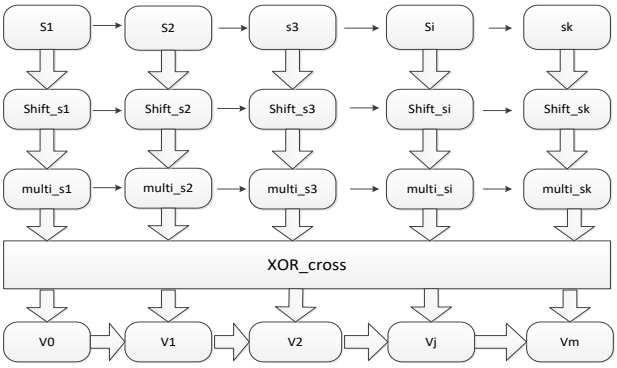


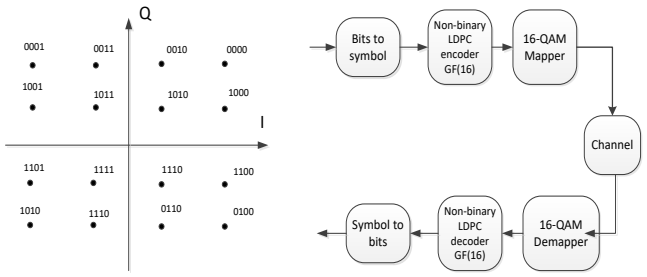
Fig .4 The Fast Encoding process to generate check sequence

For addition computation, the implementation is simple it is only based on xor unit, and multiplier can be implemented by Look-Up table.

IV. SYMBOL MODULATION AND DEMODULATION

The advantage of non-binary LDPC code outperforming 802.11n system with higher-order modulation is that it can directly match the order of the finite extension field with the constellation size. Thus, the proposed non-binary structure not only benefit from the improved code performance, but also from processing symbols instead of single bits resulting in better bandwidth efficiency. As an example to present, Fig.5(a) shows the constellation of 16-QAM with the corresponding symbol mapping based on GF(16). Each element of the finite extension filed can be directly mapped onto one of the constellation points. The number of elements in the finite extension filed equals to the number of signal points for *M*-QAM, $M=2^q$, *q* is the modulation order.

As *M* increases, the order *q* of the finite extension field and the complexity is growing too.



(a) (b)

Fig .5 (a) Mapping for 16-QAM based on Gray code: bit and symbol mapping for GF (16) generated by $g(x)=x^4+x+1$. (b) Block diagram of the system model

The system evaluation platform is shown in Fig. 5(b). The identically bits are both directly fed into an encoder applying a binary LDPC code and the reference non-binary LDPC code. In the next step, the encoded bits or symbols are mapped onto one of *M* signaling points of a square *M*-QAM. Here $X=I+j*Q$, I and Q denote the orthogonal signal respectively and can represent the set of all constellation points.

In the non-binary case, groups of 4bits are mapped onto one of the 16 points by gray code mapping with each symbol denoted as $S=[b_3,b_2,b_1,b_0]$.For the application of non-binary LDPC codes, Symbol mapping is performed by directly mapping each of the encoded symbols S onto a signaling point. At the end of the transmitter chain, the symbols are fed to the channel which is either modeled as an Additive White Gaussian Noise (AWGN) channel.

On the receiver side, a 16-QAM de-mapper generates soft information which is exploited by the subsequent channel decoder. For decoding binary LDPC codes, we apply a standard SPA based on Log-Likelihood Ratio (LLR), whereas for the non-binary case we make use of the FFT-QSPA, EMS. Because the complexity of FFT-QSPA is rather huge and FB-EMS algorithm can achieve low complexity with little performance degradation, so in this paper FB-EMS algorithm is applied.

At the end of the receiver chain, the decoded symbols are first converted to bits before being delivered.

V. NON-BINARY LDPC DECODING PROCESS BASED ON FB-EMS ALGORITHM

In the receiver side, the received symbol at time instance k is given by:$Y_k=X_k+N_k$ where N_k regarded as a complex Gaussian random noise variable with zero mean and variance. The complex Gaussian noise samples N_k are characterized by zero mean and variance $\sigma^2=\sigma_I^2+\sigma_Q^2$ and $\sigma_I^2=\sigma_Q^2$ denote the noise variances in I and Q component. In general, *I* and *Q* components are assumed to be independent of each other without any crosstalk. Therefore, the probability density function or the I and Q component of the *k-th* received symbol Y_k^I and Y_k^Q respectively can be written as

$$f\left(Y_k^I \mid X_k\right)=\frac{1}{\sqrt{\pi N_0}}\exp\left(-\frac{(Y_k^I-\mathrm{Re}\{X_k\})^2}{N_0}\right)$$

$$f\left(Y_k^Q \mid X_k\right)=\frac{1}{\sqrt{\pi N_0}}\exp\left(-\frac{(Y_k^Q-\mathrm{Im}\{X_k\})^2}{N_0}\right)$$

The probability density function of a received symbol Y_k in condition that X_k has originally been sent is then given by:

$$f\left(Y_k \mid X_k\right)=f\left(Y_k^I \mid X_k\right)*f\left(Y_k^Q \mid X_k\right)$$

So when translated into log-likelihood ratios, the equation can be rewritten as:

$$LLR(X_k=x)=LLR(X_k^I=x^I)+LLR(X_k^Q=x^Q)$$

As for decoding for non-binary LDPC code, FB-EMS algorithm is applied, the received sequences are several symbols which consist of elements in Galois Filed. For a symbol *I* received, there are *q* possible transmitted elements corresponded. All the sorted values should be subtracted the first element, the final results will not be larger than zero and the first element equals to zero. Fig.6 depicts the sorting algorithm diagram adopted in this paper. This is a kind of bubble sorting algorithm.

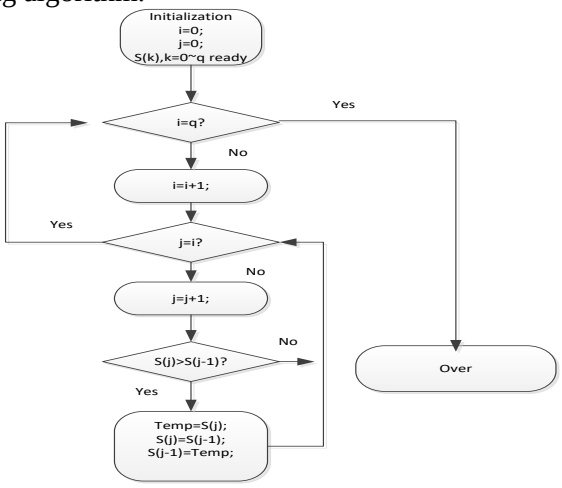


Fig .6 Bubble sorting algorithm diagram

As log-likelihood possibility can be denoted from the follow equation, each element corresponds to a log-likelihood possibility indicated as:

$$LLR\left(X_k = x\right) = \ln\frac{P_r\left(X_k = x \mid Y_k\right)}{P_r\left(X_k = \alpha \mid Y_k\right)} = \frac{\left(2Y_k - \alpha - x\right)\left(x - \alpha\right)}{2\sigma^2}$$

Where α is the most likely element for *I*. The EMS algorithm is an extension of the Min-Sum algorithm from binary to NB-LDPC codes, the decoding process for EMS is depicted as follows:

Initialization: For each received symbol, calculate its corresponding initial log-likelihood possibility:

$$f_i^x = L(X_i = x) = \log\left(\frac{P_r\left(X_i = x\right)}{P_r\left(X_i = \alpha\right)}\right)$$

$$i = 1 - N,\ j = 1 - M$$

The sorter selects most likely possible candidates for each symbol $m<<q$, as a result the decoding complexity can be reduced at large scale.

Check nodes message update: In horizon direction, for $H_{i,j} \neq 0$ calculate each symbol possibility from its corresponding equation

$$r^x{}_{i,j} = \min\Big(\sum_{H_{i,j}\otimes x + \sum_{a_x=0}^{k\neq j} H_{i,k}\otimes x'=0} q_{i,j}^x\Big)$$

Variable nodes message update: In vehicle direction, for $H_{i,j} \neq 0$, calculate each variable node message possibility from check equations except for current row:

$$q_{i,j}^x = f_i^x + \sum_{k=1,k\neq j}^{H_{i,j}\neq 0} r_{i,k}^x$$

And the final decision messages:

$$V_i^x = f_i^x + \sum_{k=1-M}^{H_{i,j}\neq 0} r_{i,k}^x$$

Make decision: For each variable node, select the maximum possibility corresponded element:

$$\hat{X}_i = \arg\max_{a\in GF(q)} V_i^x$$

Then the decoded sequence is

$$V = \left(\hat{X}_0, \hat{X}_1, \hat{X}_2 \cdots \hat{X}_{N-1}\right)$$

If $V \cdot H = 0$ the decoded sequence will be accepted, otherwise, the algorithm will return to **Check nodes message update stage** until the maximum iteration number has been reached.

For the decoding process, the check node updating unit accounts for large computation complexity. In order to reduce check node complexity, a forward-backward scheme (FB) is widely used in the check node processing for kinds of NB-LDPC decoding algorithm. The check node degree is denoted by d_c and let F_j, B_j to represent the intermediate message vector generated by the forward and backward computation, respectively. Meanwhile, *a*, *a'* and *a''* are possible code symbols. The FB contains three operations: forward, backward and merge. The FB algorithm can be described as follows:

Forward computation:

$$F_1\left(\alpha\right) = \alpha_{m,n1}(\alpha)$$

$$F_j\left(\alpha\right) = \max_{\alpha'+\alpha''=\alpha}\left(sum(F_{j-1}\left(\alpha'\right), \alpha_{m,n_j}(\alpha''))\right)$$

Backward computation:

$$B_{d_c}\left(\alpha\right) = \alpha_{m,d_c}(\alpha)$$

$$B_j\left(\alpha\right) = \max_{\alpha'+\alpha''=\alpha}\left(sum(B_{j+1}\left(\alpha'\right), \alpha_{m,n_j}(\alpha''))\right)$$

Merge computation:

$$\beta_{m,n_1}\left(\alpha\right) = B_2(\alpha),\ \beta_{m,n_{d_c}}\left(\alpha\right) = F_{d_c-1}$$

$$\beta_{m,nj}\left(\alpha\right) = \max_{\alpha'+\alpha''=\alpha}\left(sum(B_{j+1}\left(\alpha'\right), F_{j-1}(\alpha''))\right)$$

The FB-EMS aims to calculate the current symbol possibility from just to parts, one in front of current point and the other behind this point. All computation can be implemented by the same addition and comparison unit which will evidently reduce decoder complexity.

VI. Simulation Results and Analysis

The performance of proposed non-binary LDPC code system with the fast encoding algorithm in section III and FB-EMS is presented in this section VI have been simulated in this section .the performance have been compared for different value of Signal to Noise Ratio in dB at AWGN channel. (648,324) parity check matrix for 802.11n binary LDPC code based on current standard and non-binary LDPC code constructed by the method discussed in Section II are used. As for FB-EMS decoding algorithm, different truncated parameters correspond to different performance. For binary code, the code length is simple 648, when converted into non-binary one, the code is reduced to 162. The encoding process of binary or non-binary is based on the same linear structure proposed in Fig .4. For decoding process, the binary LDPC code is based on traditional sum-product algorithm presented in [3] and for non-binary LDPC code adopts FB-EMS algorithm in this paper.

Fig. 7 shows how the proposed structure non-binary LDPC code is better than its corresponding binary one for the same bit length. There is more than 1dB coding gain between non-binary LDPC code and traditional standard at 10^(-6) BER. As shown in Fig. 7 we can also conclude that with the increasing of truncated parameter the decoding performance is better but the computation complexity is also larger, so for different applications, the truncated parameter can be adaptively adjusted. In this paper, we take m=8, 4 to

illustrate.

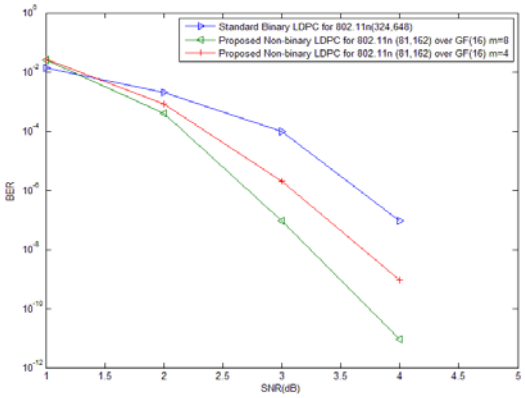


Fig .7 Comparison of traditional binary LDPC code and proposed non-binary LDPC code in AWGN Channel

VII. CONCLUSION

In this paper, we proposed a novel non-binary LDPC code over GF(16) to replace the traditional binary standard in current 802.11n system. The case for comparison is based on (648,324) code mode proposed check matrix for non-binary LDPC code is a kind of quasi-cyclic diagonal line structure which can reduce encoder complexity. The proposed matrix has been optimized to eliminate short-girths as well as low weight code-words. The process of encoding algorithm is depicted in this paper which is based on addition and multiplication computation over GF (16) and implementation can be realized by Look-Up table on the platform of ASIC or FPGA. The modulation and demodulation principle of proposed system is also presented. The decoding process for our non-binary LDPC code is based on FB-EMS which can reduce check node complexity as much as possible. At last, the error correcting performance of proposed non-binary LDPC code shows about 1dB coding gain compared with traditional binary standard. The non-binary Quasi-Cyclic LDPC with the low complexity makes our proposed system very attractive for practical purposes.

REFERENCES

[1] R.G. Gallager, Low Density Parity Check Codes, Ph.D. thesis MIT,Cambridge, Mass., September 1960.

[2] D.J.MacKay and R. Neal, “Near Shannon-limit performance of low density parity-check codes,” vol. 32, pp. 1645–1646, 1996.

[3] MC Davey and DJC MacKay, “Low density parity check codes over GF(q),” Information Theory Workshop, 1998, pp. 70–71, 1998.

[4] H. Song and J. R. Cruz, Reduced Complexity decoding of Qary LDPC codes for magnetic recording, IEEE Trans. Magn., vol. 39, pp. 1081-1087, Mar. 2003.

[5] M. Fossorier, M. Mihaljevic and H. Imai, Reduced Complexity

[6] C. Poulliat, M. Fossorier and D. Declercq, Design of Regular (2,dc)LDPC Codes over GF(q) using their Binary images, IEEE Trans.Comm.Vol. 56, no. 10, pp. 1626-1635, Oct. 2008.

[7] K. Lally and P. Fitzpatrick, “Algebraic structure of quasi-cyclic codes,“Discrete Applied Mathematics, vol. 111, no. 1-2, pp. 122–175, 2001.

[8] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, “Low complexity decoding for non-binary LDPC codes in high order fields,”IEEE Trans. Commun., vol. 58, no. 5, pp. 1365–1375, May 2010.

[9] X.-Y. Hu and E. Eleftheriou, Binary Representation of Cycle Tanner Graph GF(2^b) codes, IEEE Int. Conf. Comm. ICC’2004, June 2004.

[10] B. Zhou, J. Kang, S. Song, S. Lin, K. Abdel-Ghaffar, and M. Xu,“Construction of non-binary quasi-cyclic LDPC codes by arrays and array dispersions,” IEEE Trans. Commun., vol. 57, no. 6,pp. 1652–1662, Jun. 2009.

[11] X.Zhang and F. Cai, “Reduced-complexity decoder architecture for nonbinary LDPC codes,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 19, no. 7, pp. 1229–1238, Jul. 2011.

[12] E. Boutillon, L. Conde-Canencia and Ali AI Ghouwayel, Design of a GF(64)-LDPC Decoder Based on the EMS Algorithm, Accepted for publication in IEEE Transactions on Circuits and Systems, 2013

[13] A. Chamas AI Ghouwayel, Abbass Nasser, Ali Alaeddine and Hussein Hijazi, Statistical Analysis-Based Approach for Check Node Processor Inputs of NB-LDPC Decoder , Accepted for publication in IEEE ICCIT, June 2013.

[14] A. Chamas AI Ghouwayel, Mohamad Wehbi and Malak Mrad, Compression of LLR Messages of an Elementmy Check Node Processor of a Non-Binary LDPC Decoder , Accepted for publication in IEEE MMS2013, Spetember 2013.