



HAL
open science

Application of non-binary LDPC codes for small packet transmission in vehicle communications

Dai Kimura, Frédéric Guilloud, Ramesh Pyndiah

► **To cite this version:**

Dai Kimura, Frédéric Guilloud, Ramesh Pyndiah. Application of non-binary LDPC codes for small packet transmission in vehicle communications. ITST 2005: 5th International Conference on ITS telecommunications, Jun 2005, Brest, France. pp.109 - 112. hal-01864667

HAL Id: hal-01864667

<https://hal.science/hal-01864667>

Submitted on 30 Aug 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Application of Non-binary LDPC codes for Small Packet Transmission in Vehicle Communications

Dai Kimura^{*1}, Frédéric Guilloud^{*2} and Ramesh Pyndiah^{*2}

^{*1}Fujitsu Laboratories Limited, 5-5 Hikarino-Oka Yokosuka 239-0847, JAPAN

Phone: (+81) 468 39 5370, Fax: (+81) 468 39 5560

E-mail: dkimura@jp.fujitsu.com

^{*2}TAMCIC (UMR : CNRS 2872), ENST Bretagne, Technopôle Brest Iroise, CS 83818, 29238

BREST Cedex 3 FRANCE

Phone: (+33) 2 29 00 13 92, Fax: (+33) 2 29 00 10 12

E-mail: Frederic.Guilloud@enst-bretagne.fr, Ramesh.Pyndiah@enst-bretagne.fr

Abstract: *We propose to use non-binary low density parity check (LDPC) codes for small packet transmissions in vehicle communications. Non-binary LDPC codes which are defined by a parity check matrix over non-binary Galois field $GF(q)$ can achieve performance very close to the Shannon limit even if they are applied to small block length. By using computer simulations, we demonstrate that non-binary LDPC codes of short block length (896 bits) outperform that of binary LDPC codes and the performance can approach the Shannon limit of this block length by 0.3dB (BPSK) and less than 1.0dB (8PSK, 16QAM) at block error rate = 10^{-4} .*

Keywords: packet transmission, forward error correction (FEC), low density parity check (LDPC) code, non-binary, Galois field.

1. INTRODUCTION

Vehicle communication systems adopt small and medium size packet transmission in order to optimize system capacity which is crucial for large fleets of fast moving terminals. These small and medium size packets are subject to numerous perturbations (noise, interference) and thus powerful FEC (Forward Error Correction) is required to guarantee reliable communication. This paper deals with non-binary LDPC codes which provide an efficient solution to this coding problem.

Low density parity check (LDPC) codes were proposed by Gallager in 1962 [1]. Since their rediscovery by MacKay *et al.* in 1996 [2], research activities in this field have flourished and LDPC codes are now considered as a candidate for post turbo codes which were proposed by Berrou *et al.* in 1993 [3]. LDPC codes can achieve performance very close to the Shannon limit especially when the block length is not smaller than 10,000 [2]. For codes of shorter block length, non-binary LDPC codes have been investigated and achieve better performance [4].

An LDPC code is a linear code defined by a sparse parity check matrix \mathbf{H} . An LDPC code is called non-binary if its parity check matrix is composed of the elements of a non-binary Galois field $GF(q)$ ($q > 2$), where q denotes the order of Galois field. We often call LDPC codes over $GF(2)$ binary LDPC codes, in contrast with non-binary LDPC codes. LDPC codes can be decoded by the belief propagation algorithm on the Tanner graph associated with \mathbf{H} . The belief propagation algorithm is a sub-optimum decoding algorithm and the sparseness of \mathbf{H} enables us to decode LDPC codes efficiently by using this algorithm. Generally speaking, LDPC codes over the Galois field of higher order q can give better decoding performance. This is because non-binary LDPC codes can avoid short cycles in the Tanner graph while, at the same time, keeping Hamming weights of codewords large.

2. NON-BINARY LDPC CODES

The block diagram of non-binary LDPC codes based transmissions is shown in Fig. 1. At the transmitter, the binary data of $\log_2 q$ bits is combined to form an element of $GF(q)$ and encoded by the LDPC encoder over $GF(q)$ and then divided into binary data to be fed to the modulator. At the receiver, the received signals are demodulated to form binary probabilities of each received bit and combined to form the probabilities of each element of $GF(q)$ to be fed to the LDPC decoder over $GF(q)$.

2.1. Decoding Algorithm

The decoding of non-binary LDPC codes is performed on the Tanner graph corresponding to its parity check matrix \mathbf{H} which consists of M rows and N columns. Fig. 2 shows an example of the Tanner graph for non-binary LDPC codes which has N variable nodes, M check nodes and $MW_r = NW_c$ edges, where W_r and W_c are the average number of non-zero elements per row and per column of \mathbf{H} respectively. Each edge is

considered to have a non-binary element of $\text{GF}(q)$. In Fig. 2, h_{mn} denotes non-zero elements in \mathbf{H} . In belief propagation algorithm, decoding is performed by repeatedly exchanging probabilities between the two types of nodes [4]. The decoder stops and outputs the estimated information sequence after a fixed number of iterations or when all the parity checks are satisfied. The appendix can be referred to for more details about the decoding algorithm.

2.2. Decoding Complexity

The decoding complexity is the most significant problem for the application of non-binary LDPC codes to real systems. The direct implementation of non-binary LDPC codes exponentially increases the decoding complexity. In this case, the number of operations for each iteration is proportional to $M_b W_c q^{W_c}$, where W_c denotes the averaged weight of columns (the averaged number of non-zero elements per column) and $M_b = M \log_2 q$ denotes the number of rows of parity check matrix \mathbf{H} in binary representation.

A complexity reduction technique using Fast Fourier Transformation (FFT) has been proposed [5]. When FFT is applied to the decoding of non-binary LDPC codes, the number of operations for each iteration is proportional to $M_b W_c q$. Because the range of W_c is usually limited to $2 \leq W_c \leq 4$, the complexity is approximately proportional to the order of Galois field q for a given binary block length. This complexity can be acceptable for short block lengths.

2.3. Construction of Parity check Matrices

The decoding performance of the belief propagation algorithm converges to that of the optimum decoding such as the maximum likelihood decoding (MLD) algorithm when the Tanner graph has no cycle. A cycle means the route along the edges in the Tanner graph which starts from an arbitrary node and returns to the same node (a cycle of length 4 is highlighted in Fig. 2 by bold lines). However, it has been empirically confirmed that good asymptotic performance can be achieved even if the Tanner graph has a small number of cycles longer than 4. In this paper, we constructed parity check matrices by a random method avoiding small length cycles as few as possible, which is similar to the progressive edge growth (PEG) method [6].

The column weight distribution of parity check matrices is another important parameter for constructing good parity check matrices. It is well known that the optimized irregular weight distribution is generally better than the regular distribution [7]. It is not easy to find the optimum weight distribution especially for LDPC codes of small block length. In this paper, we use simple weight distributions which are not fully optimized. However, for non-binary LDPC codes over

the Galois field of high order, the regular and small weight distribution gives nearly optimum decoding performance [8].

Table 1 shows the parameters of all the parity check matrices that are used in the simulations whose results will be shown in the next section. In the table, "girth" denotes the minimum length of the cycles. The weight distribution gives the proportions of the number of columns of weight 2, 3 and 4. An example of a parity check matrix over $\text{GF}(256)$ is shown in Fig. 6.

3. SIMULATION RESULTS

3.1. BPSK Case

Fig. 3 shows the decoding performance of binary and non-binary LDPC codes in an AWGN channel and for a BPSK modulation. The vertical axis and horizontal axis denote block error rate (BLER) and signal to noise ratio per information bit (E_b/N_0) respectively. Six simulation results of rate 0.5 and 0.75 LDPC codes over $\text{GF}(2)$, $\text{GF}(16)$ and $\text{GF}(256)$ are shown. For a fair comparison, all codes have the same binary block length of 896. The theoretical limits calculated by using the sphere packing bound [9] are also shown. As can be seen, the decoding performance improves monotonically when the order of Galois field increases. For both code rates, the gap between the performance on $\text{GF}(256)$ and the Shannon limit is approximately 0.3 dB at $\text{BLER} = 10^{-4}$. Moreover, the binary LDPC codes over $\text{GF}(2)$ with the rate of 0.75 seems to have an error floor whereas the non-binary LDPC over $\text{GF}(256)$ does not have such a tendency.

3.2. High Order Modulation Case

For higher rate packet communications, it is useful to apply the higher order modulation such as 8PSK and 16QAM. Fig. 4 (resp. Fig. 5) shows the decoding performance of binary and non-binary LDPC codes in AWGN channel and for an 8PSK (resp. 16QAM) modulation. Though the gaps between the performance on $\text{GF}(256)$ and the Shannon limits are larger than that of BPSK, they are still less than 1.0 dB. The tendencies of error floor are almost the same as for the BPSK case.

Table 1 The parameters of the parity check matrices

GF	M	N	Weight Distribution			girth
			2	3	4	
2	448	896	0.33	0.33	0.33	8
16	112	224	0.66	0.33	0	10
256	56	112	1	0	0	10
2	672	896	0.33	0.33	0.33	10
16	168	224	0.66	0.33	0	12
256	84	112	1	0	0	18

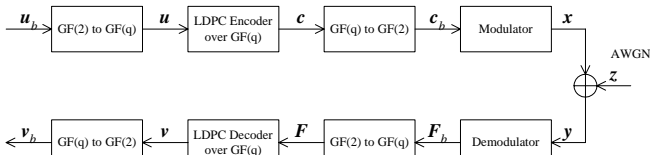


Fig. 1 Block diagram for non-binary LDPC codes based transmissions

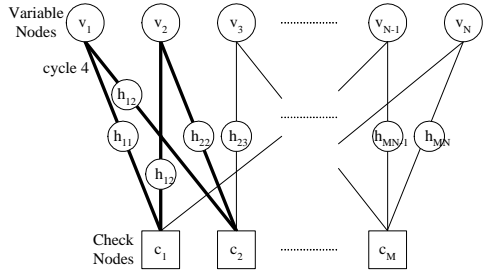


Fig. 2 Tanner graph for non-binary LDPC codes

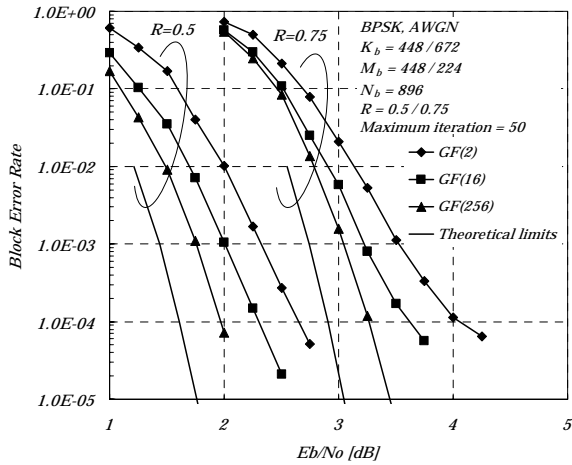


Fig. 3 Decoding performance of binary and non-binary LDPC codes (BPSK modulation)

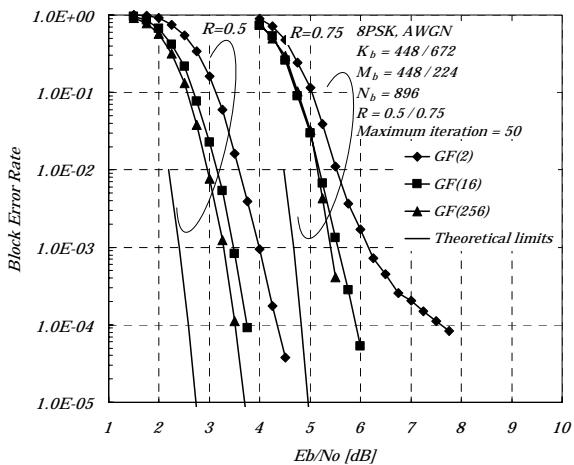


Fig. 4 Decoding performance of binary and non-binary LDPC codes (8PSK modulation)

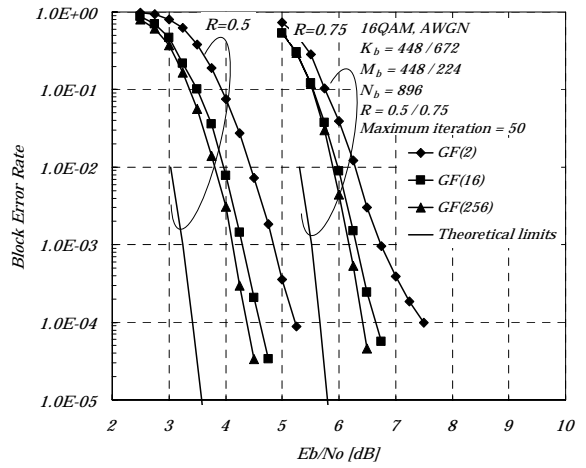


Fig. 5 Decoding performance of binary and non-binary LDPC codes (16QAM modulation)

4. CONCLUSION

Non-binary LDPC codes can give very good performance for small block length whereas binary LDPC codes of small length do not perform very well. In addition, their complexity can be reduced to the admissible level by using complexity reduction techniques such as FFT decoding. Therefore, Non-binary LDPC codes are very powerful and useful when they are applied to small and medium size packet transmissions in vehicle communications.

APPENDIX

Brief propagation algorithm for decoding of non-binary LDPC codes

The purpose of decoding is to calculate *a posteriori* probabilities (APP) over GF(q) for each symbol. Let P_n^a be the APP for the n -th symbol c_n to be equal to a ($a = 1, 2, \dots, q$). By using Bayes rule, we have

$$P_n^a = \Pr(c_n = a | \mathbf{y}) = \frac{\Pr(\mathbf{y} | c_n = a) \Pr(c_n = a)}{\Pr(\mathbf{y})}, \quad (1)$$

where \mathbf{y} and c_n denote the received modulated signal vector and the n -th encoded symbol over GF(q), respectively (See Fig. 1). We define channel value F_n^a as follows:

$$F_n^a \equiv \Pr(\mathbf{y} | c_n = a) = \sum_{c:c_n=a} \Pr(\mathbf{y} | \mathbf{c}). \quad (2)$$

In equation (1), $\Pr(c_n = a)$ is an *a priori* probability which is calculated by multiplying messages from the check nodes connected to the variable node as follows:

$$\Pr(c_n = a) = \prod_{m \in M(n)} Q_{mn}^a, \quad (3)$$

where $M(n)$ denotes the group of indices of the check nodes connected to the n -th variable node. Q_{mn}^a is the probability of $c_n = a$ from the m -th check node's point of view. Q_{mn}^a is called Q-message from the m -th check node to the n -th variable node. Q-messages are calculated as follows:

$$Q_{mn}^a = \sum_{\substack{\mathbf{c} \mathbf{h}_m^T \mathbf{c} = 0 \\ c_n = a}} \prod_{\substack{n' \in N(m) \\ n' \neq n}} R_{mn'}^{c_{n'}}, \quad (4)$$

where $N(m)$ denotes the group of indices of variable nodes connected to the m -th check node and the summation is calculated for all symbol vectors \mathbf{c} that satisfy the m -th parity check, namely $\mathbf{h}_m^T \mathbf{c} = 0$, and whose n -th element c_n is equal to a . R_{mn}^a is the probability of $c_n = a$ fed to the m -th check node from the n -th variable node. R_{mn}^a is called R-message from the n -th variable node to the m -th check node. R-messages can be calculated by using Q-messages and channel values as follows:

$$R_{mn}^a = \alpha_{mn} F_n^a \prod_{\substack{m' \in M(n) \\ m' \neq m}} Q_{m'n}^a, \quad (5)$$

where α_{mn} is the normalization factor adjusted in such a way that $\sum_{a=1}^q R_{mn}^a = 1$. In the belief propagation algorithm, Q-messages and R-messages are calculated iteratively by equations (4) and (5) in order to improve the decoding performance. Finally, we substitute converged values of Q-messages to the following equation which is given by (1), (2) and (3) to calculate the APPs.

$$\Pr(c_n = a | \mathbf{y}) = \alpha_{mn} F_n^a \prod_{m \in M(n)} Q_{mn}^a \quad (6)$$

REFERENCES

- [1] R. G. Gallager, "Low density parity check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21-28, Jan 1962.
- [2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low-density parity-check codes," *Electron. Lett.*, vol. 32, pp. 1645-1646, Aug. 1996.
- [3] C. Berrou, A. Glavieux, and Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. 1993 IEEE Int. Conf. on Communications* (Genevea, Switzerland, 1993), pp 1064-1070.
- [4] M.C. Davey and D. MacKay, "Low-Density Parity Check Codes over GF(q)," *IEEE Comm. Lett.*, Vol. 2, No. 6, Jun 1998.
- [5] L. Barnault and D. Declercq, "Fast Decoding for LDPC over GF(2^q)," *ITW2003, Paris, France*, March 31 – April 4, 2003.
- [6] X. Y. Hu, E. Eleftheriou and D. M. Arnold, "Regular and Irregular Progressive Edge-Growth Tanner Graphs," *IEEE Trans. Inform. Theory*, vol. 51, pp. 386-398, Jan. 2005.
- [7] M. C. Davey, Error-Correction Using Low-Density Parity-Check codes. PhD thesis, University of Cambridge, Cambridge, UK, Dec. 1999.
- [8] X. Y. Hu, E. Eleftheriou, "Binary Representation of Cycle Tanner-Graph GF(2^b) Codes," *Communications, 2004 IEEE International Conference on*, Vol. 1, pp528 - 532, June 2004
- [9] S. Dolinar, D. Divsalar and F. Pollara, "Code Performance as a Function of Block Size," *TMO Progress Report*. no. 42-133, May 15, 1998.

$$\mathbf{H} = \begin{bmatrix} 0 & 178 & 0 & 0 & 0 & 0 & 0 & 0 & 184 & 0 & 0 & 0 & 104 & 0 & 0 & 0 & 0 & 193 \\ 0 & 0 & 0 & 0 & 33 & 0 & 0 & 74 & 0 & 0 & 0 & 0 & 198 & 0 & 0 & 0 & 57 & 0 \\ 103 & 0 & 0 & 0 & 0 & 0 & 160 & 0 & 0 & 0 & 0 & 35 & 0 & 0 & 0 & 0 & 0 & 129 \\ 0 & 0 & 105 & 0 & 0 & 0 & 0 & 58 & 0 & 0 & 133 & 0 & 0 & 0 & 0 & 116 & 0 & 0 \\ 0 & 221 & 0 & 0 & 0 & 148 & 0 & 0 & 0 & 0 & 236 & 0 & 0 & 0 & 38 & 0 & 0 & 0 \\ 0 & 0 & 0 & 146 & 0 & 0 & 0 & 0 & 84 & 252 & 0 & 0 & 0 & 0 & 0 & 43 & 0 & 0 \\ 0 & 0 & 0 & 75 & 231 & 0 & 0 & 0 & 0 & 0 & 0 & 28 & 0 & 0 & 54 & 0 & 0 & 0 \\ 0 & 0 & 41 & 0 & 0 & 0 & 103 & 0 & 0 & 161 & 0 & 0 & 0 & 133 & 0 & 0 & 0 & 0 \\ 83 & 0 & 0 & 0 & 0 & 40 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 149 & 0 & 0 & 254 & 0 \end{bmatrix}$$

Fig. 6 An example of parity check matrix for non-binary LDPC code whose size is 9 x 18 ($M = 9, N = 18$). The column and row weights are regular ($W_c=2, W_r=3$) and the minimum cycle length is 6.