Non-Binary Low-Density Parity-Check coded Cyclic Code-Shift Keying

Oussama Abassi*, Laura Conde-Canencia*, Mohammad Mansour† and Emmanuel Boutillon*

* LabSTICC, Université Européenne de Bretagne, CNRS, UBS, Centre de Recherche, BP 92116,
56321 Lorient cedex, France
Email:{oussama.abassi,laura.conde-canencia,emmanuel.boutillon}@univ-ubs.fr

† Department of Electrical and Computer Engineering, American University of Beirut, Beirut, Lebanon
Email: mmansour@ieee.org

***Abstract*—Classically, the association of high-order modulation techniques to binary channel coding suffers from significant information loss due to the bit level channel probabilities computation. In this paper, we investigate the association of Non-Binary Low-Density Parity-Check codes (NB-LDPC) and Cyclic Code-Shift Keying (CCSK) which aims at preventing the information loss by computing the probabilities at the symbol level. Simulation results over Gaussian and Rayleigh channels demonstrate that this association leads to significant performance gains ($\approx 2.6dB$ over the Gaussian channel and $\approx 3.5dB$ over the Rayleigh channel).**

***Index Terms*—Spread spectrum communication, Parity check codes, Iterative decoding, Galois fields**

I. Introduction

Cyclic Code-Shift Keying (CCSK) [1], also known as Code-Phase-Shift Keying (CPSK), is an L-ary Direct-Sequence Spread-Spectrum (DSSS) technique that improves the spectral efficiency of spread-spectrum systems. CCSK modulation is characterized by the simplicity of the mapping and demapping operations. This property justifies the use of CCSK modulation in the Joint Tactical Information Distribution System (JTIDS) [2]. Likewise, some works are studying the possibility of using CCSK modulation in future Global Navigation Satellite Systems (GNSS) [3].

In state-of-the-art, CCSK modulation is studied in combination with binary codes. The inconvenience of this scheme is the loss of information when computing the bit probabilities. This issue is overcome by using iterative demodulation schemes that add more complexity to the receiver. This work proposes to associate CCSK modulation to Non-Binary Low-Density Parity-Check (NB-LDPC) codes. This kind of association has several advantages:

- As CCSK modulation is processed symbol-by-symbol rather than bit-by-bit, the combination with a non-binary code is directly performed without additional hardware cost.
- The soft demodulator produces uncorrelated symbol probabilities that are directly introduced in the decoder.
- The soft demodulator is easily implemented using Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) operations [4].

In [5], [6], the authors studied a similar scheme where NB-LDPC codes are combined with Orthogonal Modulation (OM) using Walsh–Hadamard sequences. In their work, soft demodulation is done using a bank of matched filters even if the Walsh-Hadamard transform would be more appropriate. In addition, they only show performance over the Gaussian channel. In this work, we first propose to implement the soft demodulator using simple FFT/IFFT operations which reduces the complexity of the receiver. On the other hand, we consider transmission over the Rayleigh block-fading channel. Simulations show that performance over the Gaussian channel and the fully interleaved Rayleigh channel are very close (a gap of only $\approx 0.2dB$ is observed).

The remainder of the paper is organized as follows. Section II presents NB-LDPC coding and decoding. Section III provides a mathematical description of CCSK modulation. Section IV describes the association of CCSK modulation and NB-LDPC codes. Simulation results are then presented in Section V. Finally, Section VI concludes the paper.

II. Non-binary LDPC codes

Denote by $\mathbb{GF}(q)$ the finite (or Galois) field of order $q = 2^p$, where $p \in \mathbb{N}_+^*$. LDPC codes are linear block codes defined by a sparse parity-check matrix H whose entries belong to a finite field $\mathbb{GF}(q = 2^p)$. If $p > 1$, they are called NB-LDPC codes. In other words, NB-LDPC codes are an extension of binary LDPC codes which aim to reduce the gap of performance with the Shannon limit when using small or moderate codeword lengths [7], [8]. The matrix H is constructed randomly and consists of N columns and M rows. N is the codeword length and M the number of parity-check equations. The number of information symbols per codeword is denoted by K. The code rate is a measure of the amount of the redundancy and is defined by $R = \frac{K}{N}$.

NB-LDPC decoders are designed with iterative message passing algorithms. The Belief Propagation (BP) [8] is one of the most efficient decoding algorithms but has very high complexity. FFT-based BP [9], log-based BP [10] and log-BP-FFT [11] were proposed to overcome the complexity of the classical BP decoder while keeping the same performance. Much effort has been dedicated to the design of suboptimal low-complexity algorithms for NB-LDPC decoding. For example, the Extended Min-Sum (EMS) algorithm [12] reduces the decoding complexity by reducing the size of the exchanged messages (at each decoding iteration, two connected nodes only exchange the n_m most reliable symbols, $n_m \ll q$). This suboptimality leads to a performance loss that can be overcome using an efficient offset correction.

III. Cyclic code-shift keying

CCSK is a DSSS modulation technique that uses 2^L waveforms to send L-bit symbols. Each waveform is a unique circular shift of a fundamental Pseudorandom Noise sequence PN whose length is equal to 2^L chips. Let $S_L = \{l, 0 \leq l \leq 2^L - 1\}$ be the set of data symbol values. The waveform PN_l associated to l, $l \in S_L$, satisfies the rule:

$$\forall i \in [0, 2^L - 1] : PN(i) = PN_l\big((i + l) \bmod 2^L\big) \quad (1)$$

The fundamental PN sequence can be generated using a Linear Feedback Shift Register (LFSR). LFSRs are known to generate maximal length sequences with good autocorrelation properties. One should note that CCSK is not orthogonal since all the sequences are derived from a unique PN signal. However, the authors in [4] showed that CCSK has close performance to OM over an AWGN channel when the symbol error probability is larger than 10^{-4}.

The CCSK soft demodulation is performed by computing the cross-correlation vector between the received signal and all the possible sequences. This task can be achieved using a bank of matched filters as suggested in [1]. Nevertheless, a more convenient implementation is to compute the cross-correlation by applying FFT and IFFT operations.

IV. NB-LDPC coded CCSK modulation

This section presents the association of CCSK modulation to NB-LDPC codes which aims at better exploiting the good error correcting capabilities of this family of codes by preventing the loss of information at the soft demodulation. The system model is illustrated in Fig. 1.

A. The transmitter model

At the transmitter, message bits are grouped into p-bit symbols and then encoded by an NB-LDPC encoder to generate the codeword. After that, a p-ary CCSK encoder associates the appropriate waveform signal to each codeword symbol by right-shifting the fundamental PN sequence. The Galois field is constructed by taking a root α of an irreducible polynomial over $\mathbb{GF}(2)$. The null element is directly mapped to PN. The other $\mathbb{GF}(q = 2^p)$ elements are mapped according to the following rule:

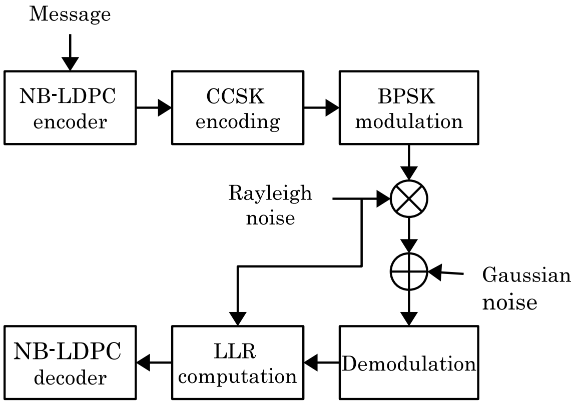

Fig. 1. Block diagram of NB-LDPC coded CCSK modulation

$$\forall k \in [0, q-2] : CCSK(\alpha^k) = PN_{k+1} \quad (2)$$

At the back end, the chip modulation is done using Binary Phase-Shift Keying (BPSK).

B. Demodulation and log-likelihood ratios computation

Let us denote $Y = [y_i]_{0 \leq i \leq q-1}$ the transmitted CCSK signal associated to a given codeword symbol and $Z = [z_i]_{0 \leq i \leq q-1}$ the received sequence corresponding to Y. Assuming a frequency nonselective Rayleigh fading channel, Z is given by:

$$\forall i \in [0, q-1] : z_i = \gamma_i y_i + \delta_i \quad (3)$$

where δ_i is a realization of a white Gaussian noise of variance σ^2, and γ_i is a realization of a Rayleigh noise characterized by the following probability density function:

$$\forall \gamma_i \in \mathbb{R}_+^* : P(\gamma_i) = 2\gamma_i e^{-\gamma_i^2} \quad (4)$$

$\Gamma = [\gamma_i]_{0 \leq i \leq q-1}$ is the set of Rayleigh noise factors corresponding to Z. If $\forall i \in [0, q-1] : \gamma_i = 1$, the channel is an Additive White Gaussian Noise (AWGN) channel.

Assuming ideal Channel State Information (CSI) at the receiver, the Log-Likelihood Ratio (LLR) is given by:

$$\begin{aligned} \forall k \in [0, q-2] : LLR\left(\alpha^k\right) &= \ln\left(\frac{P\big(Z|(\Gamma, \alpha^k)\big)}{P\big(Z|(\Gamma, 0)\big)}\right) \\ LLR(0) &= 0 \end{aligned} \quad (5)$$

$\forall k \in [0, q-2]$, $Y^{k+1} = [y_i^{k+1}]_{0 \leq i \leq q-1}$ denotes the CCSK sequence corresponding to α^k, and $Y^0 = [y_i^0]_{0 \leq i \leq q-1}$ denotes the one corresponding to the null symbol. Thus, the LLR can be written as follows:

$$LLR\left(\alpha^k\right) = \ln\left(\frac{P\big(Z|(\Gamma, Y^{k+1})\big)}{P\big(Z|(\Gamma, Y^0)\big)}\right) \quad (6)$$

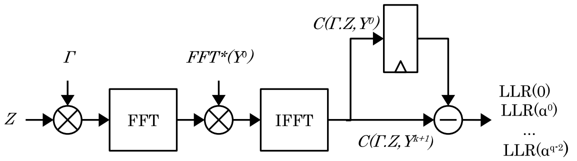

Fig. 2. LLR computation circuit

Assuming independent distribution of errors, we get:

$$LLR\left(\alpha^k\right) = \ln\left(\frac{\prod_{i=0}^{q-1} P\big(z_i|(\gamma_i, y_i^{k+1})\big)}{\prod_{i=0}^{q-1} P\big(z_i|(\gamma_i, y_i^{0})\big)}\right) \tag{7}$$

Next, given that:

$$P\big(z_i|(\gamma_i, y_i^{k+1})\big) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(z_i - \gamma_i y_i^{k+1})^2}{2\sigma^2}\right) \tag{8}$$

it follows that:

$$LLR\left(\alpha^k\right) = \frac{1}{\sigma^2}\sum_{i=0}^{q-1}\left(\gamma_i y_i^{k+1} z_i\right) - \frac{1}{\sigma^2}\sum_{i=0}^{q-1}\left(\gamma_i y_i^{0} z_i\right) \tag{9}$$

If the EMS decoding algorithm is used, the LLR expression can be simplified without affecting the performance by omitting the $\frac{1}{\sigma^2}$ common factor:

$$LLR\left(\alpha^k\right) = \sum_{i=0}^{q-1}\left(\gamma_i y_i^{k+1} z_i\right) - \sum_{i=0}^{q-1}\left(\gamma_i y_i^{0} z_i\right) \tag{10}$$

Let us denote $C\left(\Gamma Z, Y^{k+1}\right) = \sum_{i=0}^{q-1}\left(\gamma_i y_i^{k+1} z_i\right)$ and $C\left(\Gamma Z, Y^{0}\right) = \sum_{i=0}^{q-1}\left(\gamma_i y_i^{0} z_i\right)$. Note that each of $C\left(\Gamma Z, Y^{k+1}\right)$ and $C\left(\Gamma Z, Y^{0}\right)$ is the cross-correlation of a given CCSK sequence and the received signal Z scaled by Γ. Therefore, as mentioned in Section III, it is more convenient to use FFT/IFFT operations to compute equation (10). The LLR computation circuit is illustrated in Fig. 2. The normalization term $C\left(\Gamma Z, Y^{0}\right)$ is first saved in a register and then subtracted from the remaining outputs of the IFFT circuit.

V. Simulation Results

We consider performance of $\mathbb{GF}(64)$-LDPC coded CCSK modulation. Monte-Carlo simulations were performed using regular NB-LDPC codes that were designed within the framework of the European DAVINCI project [13]. The codewords are randomly generated so that the joint demodulator–decoder is independent of the transmitted codeword. In the remainder of this section, K and N are expressed in bits. The PN sequence consists of 64 chips generated using an LFSR of size 6 chips defined by the primitive polynomial $Q\left(x\right) = x^6 + x + 1$. More specifically, the LFSR generates a periodic sequence of 63 chips that has excellent autocorrelation properties; then an additional chip is inserted to obtain the 64-length sequence. Therefore, the corresponding autocorrelation function is slightly altered. On the receiver side, the simulations were performed by the EMS algorithm in addition to the BP algorithm because the latter has no practical interest. On the one hand, the BP decoder has been implemented using the log-BP-FFT scheme due to its reduced complexity compared to the straightforward scheme. On the other hand, the EMS decoder has been implemented by fixing the size of the truncated messages to $n_m = 24$ and the value of the correction offset to 1. For both decoders the maximum number of decoding iterations is fixed to 100.

In Fig. 3, several $\mathbb{GF}(64)$-LDPC coded CCSK modulation schemes with different code lengths are compared to the Shannon theoretical limit of equivalent finite length codes [14]. To make the comparison fair, the spectral efficiency of the coded CCSK modulation should be taken into account. Thus, the value of the code rate used to compute the Shannon limit is equal to the rate of the corresponding $\mathbb{GF}(64)$-LDPC code multiplied by the CCSK modulation rate (i.e. $R \cdot \frac{6}{64}$). At $FER = 10^{-4}$ we observe a gap of $\approx 1dB$ with the Shannon limit for the three considered codelengths.

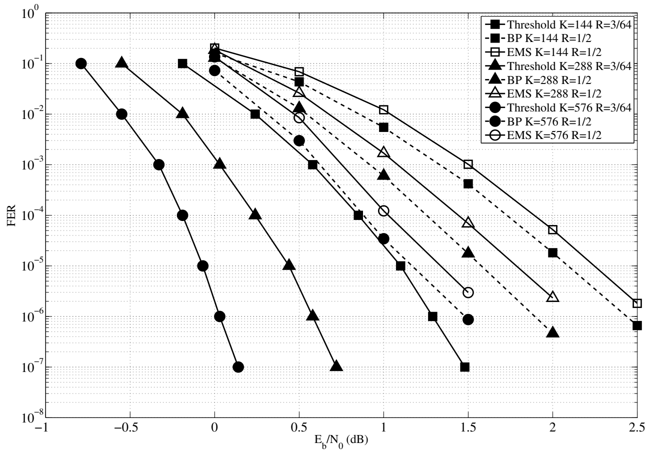

Fig. 3. FER performance of NB-LDPC coded CCSK modulation over the AWGN channel.

Fig. 4 shows that $\mathbb{GF}(64)$-LDPC coded CCSK modulation and $\mathbb{GF}(64)$-LDPC coded OM (using Sylvester constructed Hadamard matrix of order 64) have nearly the same performance over the AWGN channel. Therefore, non binary coded CCSK is an attractive choice because of its low implementation cost. Fig. 4 also shows the performance of binary LDPC codes constructed using the Progressive Edge Growth (PEG) algorithm [15], [16]. PEG codes have demonstrated good performance for small block lengths. The simulation of the PEG codes is done using the Min-Sum decoding algorithm and a maximum number of decoding iterations equal to 500. As can be observed, the performance of the PEG-LDPC coded CCSK modulation is worse than the PEG-LDPC coded BPSK modulation. The observed degradation is due to the loss of information in the calculation of the bit LLR values. In contrast, the performance of the $\mathbb{GF}(64)$-LDPC coded CCSK modulation is significantly improved compared to the $\mathbb{GF}(64)$-LDPC coded BPSK modulation. In this case, the decoder fully benefits from the time diversity introduced by the CCSK modulation because the demodulation is done without loss of information.

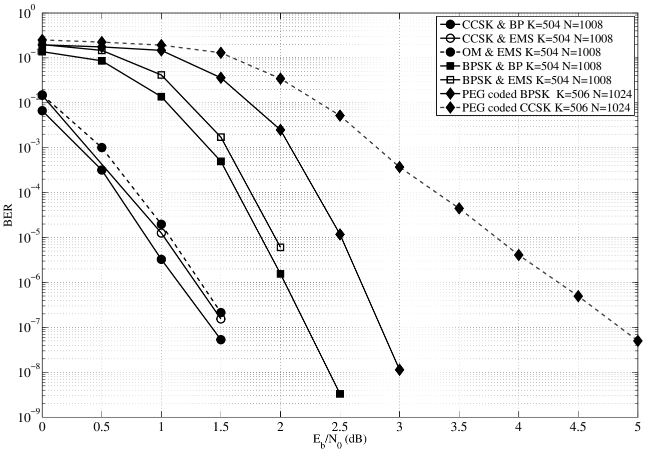

Fig. 4. BER performance of NB-LDPC coded CCSK modulation over the AWGN channel.

Fig. 5 shows the performance of $\mathbb{GF}(64)$-LDPC coded CCSK modulation over the Rayleigh block-fading channel. In such a channel, the fading remains constant within the same block of transmitted chips (or bits) but is independent from block to block. The number of chips (or bits) per block is denoted by n_b. A realistic model of that channel can be obtained by an interleaved Orthogonal Frequency-Division Multiplexing (OFDM) scheme. Using an ideal chip interleaver ($n_b = 1$ chip), the performance of the $\mathbb{GF}(64)$-LDPC coded CCSK modulation is close to its performance over the AWGN channel (a gap of $\approx 0.2dB$ is observed between the two curves). Note that such surprising result is due to the fact that:

- The diversity of the channel is equal to the total number of transmitted chips (i.e. $\frac{N}{6} \cdot 64$).
- The receiver is fully able to benefit from the diversity of the channel.

For comparison purposes, n_b is fixed to 11 chips for the $\mathbb{GF}(64)$-LDPC coded CCSK modulation and to 1 bit for the PEG-LDPC coded CCSK modulation, so that the two schemes have roughly the same diversity order (i.e. N for the PEG code and $\frac{N \cdot 64}{66}$ for the DAVINCI code). At $BER = 10^{-4}$, a gap of $\approx 3.5dB$ is observed between the two curves. Even by reducing the channel diversity ($n_b = 64$ chips), the performance of the $\mathbb{GF}(64)$-LDPC coded CCSK modulation remains better at the low SNR region but has a lower slope.

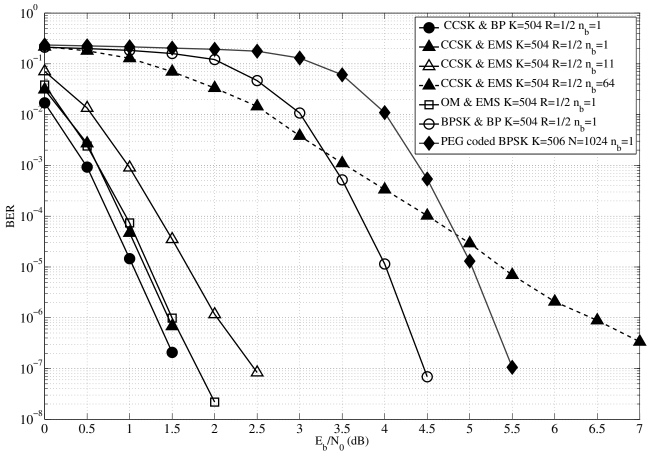

Fig. 5. BER performance of NB-LDPC coded CCSK modulation over the Rayleigh channel.

VI. Conclusion

In this paper, the use of NB-LDPC codes as a non binary coding scheme for CCSK modulation has been proposed. The combination is straightforward and adds no hardware complexity to the transmitter. The soft demodulation is simplified and can be performed using FFT/IFFT operations. Furthermore, LLR values are computed without loss of information which benefits the decoder from the diversity introduced by the CCSK modulation. Monte-Carlo simulations show that performance is significantly improved, which renders the presented scheme an attractive solution for systems requiring low transmission power such as sensor networks. In addition, since CCSK is designed to increase the transmission bit rate of a spread spectrum signal, non-binary coded CCSK modulation is a potential candidate for future GNSS systems. Finally, future work will be dedicated to show the benefits of non binary coded CCSK modulation with Single-Carrier Frequency-Domain-Equalization (SC-FDE) systems [17].

VII. Acknowledgment

Special thanks to D. J. C. MacKay from University of Cambridge and Xiao-Yu Hu from IBM Zurich Research Laboratory for supplying the source code for PEG construction. The authors would also like to thank J. Le Masson from Écoles de Saint-Cyr Coëtquidan for his pertinent remarks.

References

[1] A. Y.-C. Wong and V. C. M. Leung, "Code-phase-shift keying: a power and bandwidth efficient spread spectrum signalling technique for wireless local area network applications," in *Proc. IEEE Canadian Conf. Elect. Comput. Eng.*, vol. 2, May 1997, pp. 478–481.

[2] C.-H. Kao, C. Robertson, and K. Lin, "Performance analysis and simulation of cyclic code-shift keying," in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, nov. 2008, pp. 1 –6.

[3] A. G. Peña, M.-L. Boucheret, C. Macabiau, J.-L. Damidaux, L. Ries, S. Corazza, and A.-C. Escher, "Implementation of code shift keying signalling technique in galileo e1 signal," in *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, dec. 2010, pp. 1 –8.

[4] G. M. Dillard, M. Reuter, J. Zeidler, and B. Zeidler, "Cyclic code shift keying: a low probability of intercept communication technique," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 3, Jul. 2003.

[5] Y. zhen Huang, Y. peng Cheng, Y. ming Zhang, G. hai Yu, and J. Chen, "Combine non-binary LDPC codes with m-ary orthogonal spread spectrum modulation," in *Wireless Communications and Signal Processing (WCSP), 2010 International Conference on*, oct. 2010, pp. 1 –4.

[6] S. Lin, M. R. Masse, M. B. Pursley, T. C. Royster, and S. Song, "Frequency-hop antijam communications with nonbinary error-control coding," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, oct. 2007, pp. 1 –7.

[7] R. G. Gallager, "Low-density parity-check codes," Ph.D. dissertation, MIT, Cambridge, Mass., Sep. 1960.

[8] M. Davey and D. J. C. MacKay, "Low density parity check codes over $\mathbb{GF}(q)$," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.

[9] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over $\mathbb{GF}(2^q)$," in *Proc. IEEE Inf. Theory Workshop*, Mar./Apr. 2003, pp. 70–73.

[10] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over $\mathbb{GF}(q)$," in *Proc. IEEE Int. Conf. Commun.*, vol. 2, Jun. 2004, pp. 772–776.

[11] H. Song and J. R. Cruz, "Reduced-complexity decoding of *Q*-ary LDPC codes for magnetic recording," *IEEE Trans. Magn.*, vol. 39, no. 2, pp. 1081–1087, Mar. 2003.

[12] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over $\mathbb{GF}(q)$," *IEEE Trans. Commun.*, vol. 55, no. 4, pp. 633–643, Apr. 2007.

[13] I. Gutierrez, G. Bacci, J. Bas, A. Bourdoux, H. Gierszal, A. Mourad, and S. Pleftschinger, "Davinci non-binary LDPC codes: Performance and complexity assessment," in *Future Network and Mobile Summit, 2010*, june 2010, pp. 1 –8.

[14] E. Maury. Theoretical performance limit evaluation. [Online]. Available: http://departements.telecom-bretagne.eu/data/elec/turbo/LIMIT/

[15] D. J. C. MacKay. Source code for progressive edge growth parity check matrix construction. [Online]. Available: http://www.inference.phy.cam.ac.uk/mackay/PEG_ECC.html

[16] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Progressive edge-growth tanner graphs," in *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE*, vol. 2, 2001, pp. 995 –1001 vol.2.

[17] F. Pancaldi, G. Vitetta, R. Kalbasi, N. Al-Dhahir, M. Uysal, and H. Mheidat, "Single-carrier frequency domain equalization," *Signal Processing Magazine, IEEE*, vol. 25, no. 5, pp. 37 –56, september 2008.