Non-Binary Coded CCSK and Frequency-Domain Equalization with Simplified LLR Generation

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-In this paper, we investigate the performance of Single-Carrier (SC) transmission with Non-Binary Low-Density Parity-Check (NB-LDPC) coded Cyclic Code-Shift Keying (CCSK) signaling in a multipath environment and we show that the combination of CCSK signaling and non-binary codes results in two key advantages, namely, improved Log-Likelihood Ratio (LLR) generation via correlations and reduced implementation complexity. We demonstrate that Maximum Likelihood (ML) demodulation can be expressed by two circular convolution operations and thus it can be processed in the frequency domain. Then, we propose a joint Frequency-Domain Equalization (FDE) and LLR generation scheme that aims at reducing the complexity of the receiver. Finally, we demonstrate through Monte-Carlo simulations and histogram analysis that this proposed CCSK signaling scheme gives more robustness to SC-FDE systems than commonly employed Hadamard signaling schemes (a gap of $\approx 1.5dB$ in favor of CCSK signaling is observed at $BER = 10^{-3}$ assuming perfect Channel State Information).

Index Terms—Equalizers, Iterative decoding, Parity check codes, Spread spectrum communication

I. INTRODUCTION

Cyclic Code-Shift Keying (CCSK) [1] is an 2^M -ary direct-sequence spread-spectrum technique that associates 2^M -chip sequences to M-bit symbols. The CCSK sequences are all derived from a unique pseudo-random noise sequence by circular shifts. CCSK signaling is already employed in the Joint Tactical Information Distribution System (JTIDS) [2], and is a candidate for adoption in future Global Navigation Satellite Systems (GNSS) [3].

In this paper, we investigate the robustness of Single-Carrier (SC) transmission with CCSK signaling and non-binary coding over a multipath channel. The association of a high-order modulation and a non-binary code avoids the performance loss because Log-Likelihood Ratio (LLR) values are generated directly at the symbol level. In the proposed scheme, LLRs are generated by calculating the correlation between the received signal and the set of CCSK sequences. Furthermore, this task is performed in the frequency domain using Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) blocks, which reduces the receiver complexity [4]. The association of

CCSK and non-binary codes is straightforward and does not add hardware complexity to the transmitter [5].

In a multipath channel, the mobile terminal receives different replicas of the same signal with different amplitudes and phases, which causes time dispersion and InterSymbol Interference (ISI). We first show that a Maximum Likelihood (ML) demodulator simply consists of two circular convolution blocks that can be efficiently implemented using FFT and IFFT operations. Furthermore, we investigate the issue of Frequency Domain Equalization (FDE). Hence we consider in this work as well the case of Minimum Mean-Square Error (MMSE) equalization, which can also be implemented using FFT/IFFT blocks. Thus, both LLR computation and channel equalization are performed using a single FFT/IFFT block which, indeed, simplifies the receiver complexity. Although a similar idea is proposed in [6], we claim the intellectual property right since we applied for a French patent [7] before [6] was published. In addition, the latter mentioned paper does not investigate the advantages of using CCSK signaling to boost the performance of non-binary codes.

The rest of the paper is organized as follows. Section II describes the association of the non-binary coded CCSK and SC-FDE. Section III gives simulation results. Finally, Section IV gives some concluding remarks.

II. ASSOCIATION OF NB-LDPC CODED CCSK AND CHANNEL EQUALIZATION

In this section, we first show that, in SC transmission including non-binary coded CCSK, ML demodulation consists of two circular convolution operations. Then, for SC transmission with an MMSE equalizer we show that both equalization and LLR computation can be performed using a single FFT/IFFT block (nevertheless, MMSE can be replaced by other linear equalization schemes).

A. NB-LDPC codes

An NB-LDPC code is a block code defined over a Galois field $GF(q=2^M)$ and characterized by a sparse parity

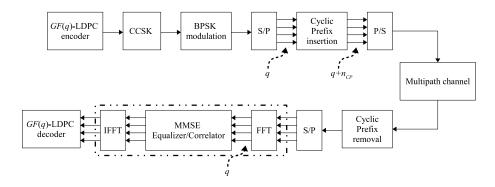


Fig. 1. SC-FDE and NB-LDPC coded CCSK

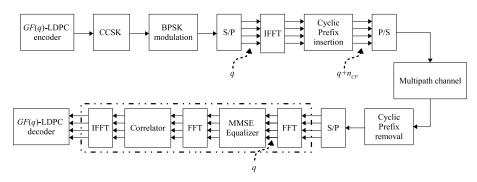


Fig. 2. OFDM and NB-LDPC coded CCSK

check matrix. These codes are known to have good error correction performance for short and moderate code lengths [8]. Decoding is performed iteratively using the Belief Propagation (BP) algorithm. However, this algorithm has very high complexity. Alternative sub-optimal decoding algorithms with reduced complexity were derived in the literature, such as the Extended Min-Sum (EMS) or the Min-Max algorithms. Recently, a practical implementation of the EMS decoder over GF(64) was proposed within the DAVINCI European project [9].

B. ML demodulation for SC transmission and non-binary coded CCSK

At the transmitter, message bits are grouped into M-bit symbols and then encoded by a $GF(q=2^M)$ -LDPC encoder to generate the codeword. Subsequently, each symbol of the codeword is associated with a CCSK sequence. Let pn denote the fundamental q-chip pseudo-noise random sequence, where $pn(i) \in \{-1,1\}, i=0,\cdots,q-1$, and let α_k , $k=0,\cdots,q-1$, be the symbols of GF(q). Each symbol α_k is associated with a CCSK sequence (denoted by y_{α_k}) by a K-position circular shift of pn:

$$y_{\alpha_k}(i) = pn((i+k)_q), i = 0, \cdots, q-1$$
 (1)

where $(.)_q$ is the modulo-q operator.

The ISI is confined in cyclic prefixes corresponding to the last $n_{\rm cp}$ chips of the transmitted CCSK sequence (we set $n_{\rm cp}$ equal to the maximum channel delay). Each cyclic prefix separates two consecutive transmitted CCSK sequences.

Denote by h the multipath Channel Impulse Response (CIR) $(h(i)=0, \forall i\geq n_{\rm cp})$. After removing the cyclic prefix, the received samples z(i) corresponding to a transmitted symbol α_k are given by:

$$z(i) = (y_{\alpha_k} \otimes_q h)(i) + n(i)$$

$$= \sum_{j=0}^{q-1} y_{\alpha_k} ((i-j)_q) \cdot h(j) + n(i)$$

$$= \sum_{j=0}^{q-1} pn((i+k-j)_q) \cdot h(j) + n(i)$$
(2)

where \otimes_q denotes circular convolution modulo-q, and n is a complex Gaussian noise distributed with zero mean and standard deviation

$$\sigma = \sqrt{\frac{1}{2 \cdot R \cdot \frac{M}{q + n_{cp}} \cdot 10^{\frac{\left(\frac{E_b}{N_0}\right)}{10}}}}$$
(3)

where R is the code rate and $\frac{E_b}{N_0}$ is the ratio of energy per bit to noise power measured in decibels. The ratio $\frac{M}{q+n_{\rm cp}}$ can be viewed as the coding rate of the CCSK modulation scheme, where M bits of information are transmitted on $q+n_{\rm cp}$ chips.

Assuming all symbols are equiprobable, then the LLR of the symbol $\alpha_{k'}$ is given by:

$$LLR(\alpha_{k'}) = \ln\left(\frac{P(z\backslash\alpha_{k'})}{P(z\backslash\alpha_{0})}\right)$$
$$= \ln\left(\frac{P(z\backslash y_{\alpha_{k'}})}{P(z\backslash y_{\alpha_{0}})}\right) \tag{4}$$

where $P(a \setminus b)$ is the conditional probability distribution of a given b. Furthermore, assuming independent distribution of errors and perfect Channel State Information (CSI) we get:

$$LLR(\alpha_{k'}) \propto Real\left(\sum_{i=0}^{q-1} z(i) \cdot (y_{\alpha_{k'}} \otimes_q h^*)(i)\right)$$
$$-Real\left(\sum_{i=0}^{q-1} z(i) \cdot (y_{\alpha_0} \otimes_q h^*)(i)\right)$$
(5)

where Real(.) and $(.)^*$ are the complex real part and the complex conjugate, respectively. By noting that the second term in (5) is a special case of the first term when k'=0, we focus hereafter on the first term and expand it to

$$T \triangleq \sum_{i=0}^{q-1} z(i) \cdot \left(y_{\alpha_{k'}} \otimes_q h^* \right) (i)$$
$$= \sum_{i=0}^{q-1} \left(z(i) \cdot \sum_{j=0}^{q-1} pn \left((i+k'-j)_q \right) \cdot h^*(j) \right) \quad (6)$$

Since the addition operation is commutative, we can index the terms in a circular fashion by writing $i=(m-k')_q$, where m runs from 0 to q-1. Therefore, we obtain the following equivalent expression:

$$T = \sum_{m=0}^{q-1} \left(z \left((m-k')_q \right) \cdot \sum_{j=0}^{q-1} pn \left((m-j)_q \right) \cdot h^*(j) \right)$$
$$= \left(z \otimes_q (pn \otimes_q h^*) \right) (k')$$
 (7)

Equation (7) shows that ML demodulation consists entirely of circular convolutions. Therefore, LLRs can be computed in the frequency domain which reduces the complexity of the receiver.

C. Association of NB-LDPC coded CCSK and SC-FDE

SC-FDE is a single carrier transmission scheme used to mitigate the ISI while avoiding the drawbacks of OFDM [10]. Figure 1 shows a SC-FDE system including NB-LDPC coded CCSK. An $n_{\rm cp}$ -chip cyclic prefix is added at the beginning of each transmitted CCSK sequence. This way, CCSK sequences would then be circularly convolved with the CIR. Therefore, the receiver can process separably each sequence after removing the cyclic prefixes. In other words, the received signal is equalized in the frequency domain sequence by sequence. Furthermore, the FDE and the LLR computation can be performed using the same FFT/IFFT block. Without loss of generality, we use MMSE equalization [11] to describe

the proposed receiver. Denote by H the q-point FFT of h. Then the i-th MMSE equalizer coefficient $\beta(i)$ is given by:

$$\beta(i) = \frac{(H(i))^*}{|H(i)|^2 + \sigma^2}, i = 0, \dots, q - 1$$
 (8)

where | . | denotes complex magnitude.

Denote by PN and Z the q-point FFTs of pn and z, respectively. The output vector W_{SC} of the MMSE equalizer/correlator block is given by:

$$W_{SC}(i) = PN(i) \cdot \beta(i) \cdot Z(i), i = 0, \cdots, q - 1$$
 (9)

The correlation vector, denoted by w_{SC} between the equalized signal and the q CCSK sequences is obtained by applying a q-point IFFT to W_{SC} . Thus, the LLR of a symbol $\alpha_{k'}$ is given by:

$$LLR(\alpha_{k'}) = w_{SC}(k') - w_{SC}(0). \tag{10}$$

D. Association of NB-LDPC coded CCSK and OFDM

In the case of OFDM, the factorization of the FFT/IFFT blocks is not possible because at the transmitter the OFDM symbols are generated by applying an IFFT to the time-domain signal. Therefore, the receiver requires an additional FFT between the MMSE equalizer and the correlator blocks as shown in Fig. 2. Formally, the i-th MMSE equalizer coefficient $\beta(i)$ is given by:

$$\beta(i) = \frac{(H(i))^*}{|H(i)|^2 + q \cdot \sigma^2}, i = 0, \dots, q - 1$$
 (11)

The output vector W_{OFDM} of the MMSE equalizer is given by:

$$W_{\text{OFDM}}(i) = \beta(i) \cdot Z(i), i = 0, \cdots, q - 1$$
 (12)

Denote by \tilde{W}_{OFDM} the q-point FFT of W_{OFDM} . The output of the correlator block, denoted by \hat{W}_{OFDM} is thus given by:

$$\hat{W}_{\text{OFDM}}(i) = PN(i) \cdot \tilde{W}_{\text{OFDM}}(i), i = 0, \cdots, q - 1$$
 (13)

If \hat{w}_{OFDM} is the q-point IFFT of \hat{W}_{OFDM} , the LLR of a symbol $\alpha_{k'}$ is given by:

$$LLR(\alpha_{k'}) = \hat{w}_{OFDM}(k') - \hat{w}_{OFDM}(0). \tag{14}$$

As a conclusion, it is apparent that the receiver complexity of SC-FDE is reduced compared to OFDM. First, the factorization of the FFT/IFFT blocks is only feasible for SC-FDE. Second, if we assume that the channel is constant during a transmitted frame, and according to equations (9), (12), (13), LLR computation and channel equalization are performed using one multiplication per sample in SC-FDE but require two multiplications per sample in the case of OFDM.

III. SIMULATION RESULTS

We consider the Channel Model A [12] that was specified to describe a typical office NLOS environment in the LTE standard. This channel is characterized by a Finite Impulse Response (FIR) where each tap suffers an independent Rayleigh fading with an average power following an exponentially decaying Power Delay Profile (PDP). The Root Mean Square (RMS) delay spread is fixed to $\tau=50~ns$ and the sampling period to $T_s=50~ns$. In our simulations, we fix the maximum channel delay to $10\cdot\tau$. The maximum number of paths is then obtained by $n_{path}=\frac{10.\tau}{T_s}$. We determine the power of the first tap so as to make the average received power equal to one.

We use an NB-LDPC code developed within the framework of the DAVINCI project [13]. This code is defined over GF(64). The codeword length is N=1008 bits and the code rate is $R=\frac{1}{2}$. Decoding is performed using the EMS algorithm. The truncated messages are of size $n_m=24$, the correction offset is fixed to 0.2 and the maximum number of iterations is set to 21.

CCSK sequences are of size 64 chips. The pn sequence is constructed as follows: we first generate a maximal length sequence of size 63 chips. For this purpose, we use an LFSR defined by the polynomial $Q(x) = x^6 + x + 1$. Then, we add to this sequence one additional chip to obtain pn.

In [14], a transmission scheme combining NB-LDPC codes and M-ary Orthogonal spread-spectrum Modulation (OM) was proposed and evaluated over the Additive White Gaussian Noise (AWGN) Channel. Hereafter, we extend the evaluation of that scheme to multipath environment to make comparison with our scheme. The OM sequences are generated using a Sylvester Hadamard matrix of order 64 [15].

To have a fair comparison, both SC-FDE and OFDM use FFT/IFFT of size 64. An OFDM symbol is obtained by applying an IFFT to a CCSK sequence (i.e. the number of data sub-carriers is 64 and we do not use pilot sub-carriers).

The used binary LDPC code is constructed with the progressive edge growth (PEG) algorithm [16]. PEG codes have demonstrated good performance for small block lengths. The codeword length is N=1024 bits and the code rate is $R=\frac{506}{1024}\approx 0.49$. We consider the Min-Sum algorithm with a maximum number of decoding iterations fixed to 100. The simulation is done by grouping bits into blocks of n_b bits. Then, each bit in each block is mapped into a CDMA signal of n_c chips. Finally, we add to each block a cyclic prefix. n_b and n_c must satisfy $n_b \cdot n_c = 64$ to obtain the same diversity of NB-LDPC coded CCSK. Furthermore, because NB-LDPC symbols are composed of 6 bits, we used $n_b = 4$ bits and $n_b = 8$ bits so that the spectral efficiency of the NB-LDPC coded CCSK is enclosed between the spectral efficiencies of the two simulated binary LDPC coded CDMA schemes.

The cyclic prefixes used for all simulated schemes are of size $n_{\rm cp}=n_{path}=11$ chips such that two consecutive transmitted sequences are completely independent from each other.

All simulations are performed with random codewords and

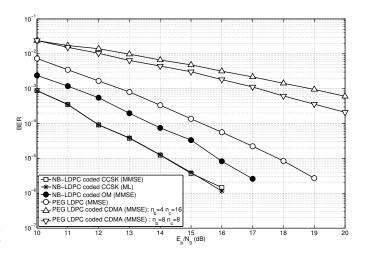


Fig. 3. BER performance of NB-LDPC coded CCSK combined with SC-FDE (Channel Model A)

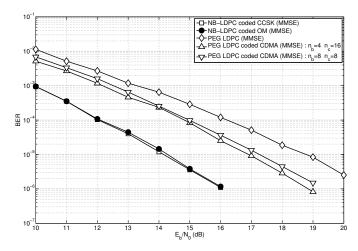


Fig. 4. BER performance of NB-LDPC coded CCSK combined with OFDM (Channel Model A)

random realizations of the channel. In addition, we assume that the CIR remains constant during each transmitted codeword.

Fig. 3 and Fig. 4 show the BER obtained for SC-FDE and OFDM, respectively. We first note that ML demodulation and MMSE equalization give similar performance in SC transmission. Second, we note that CCSK has almost similar performance in both SC-FDE and OFDM systems. However, while OM and CCSK have similar performance in OFDM, the performance of OM significantly decreases in SC-FDE. To explain this surprising result, we ran the code shown in Algorithm 1.

The negative values of Δ give an approximate estimation of the hard demodulation Symbol Error Rate (SER). Fig. 5 shows the superimposed histograms of CCSK and Hadamard sequences obtained for an $\frac{E_b}{N_0} \approx 15~dB$. We observe that the negative surface of Δ is larger for Hadamard signaling which leads to better decoding performance in favor of CCSK signaling (it is well known that the performance of a non-binary decoder essentially depends on its input SER). To

Algorithm 1 Experiment to demonstrate the robustness of non-binary coded CCSK signaling with respect to non-binary coded Hadamard signaling in a multipath environment.

for i = 0 to 63 do

for j = 1 to 10000 do

- y_{α_i} denotes the *i*-th CCSK sequence (or the *i*-th Hadamard sequence). Transmit y_{α_i} over a random realization of the multipath channel
- Equalize the received signal to obtain z_{α_i}
- c_k denotes the correlation of z_{α_i} with y_{α_k} . Calculate $c_k, k=0,\cdots,q-1$
- Compute the difference $\delta = c_i \max_{k \in [0.63] \setminus \{i\}} \left\{ c_k \right\}$
- Update the vector $\Delta = \Delta \cup \delta$

end for

end for

Plot the histograms of Δ for both CCSK and Hadamard signaling

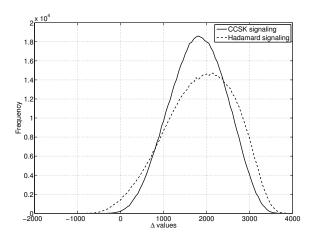


Fig. 5. Histograms of Δ for CCSK and Hadamard signaling over Channel Model A $(\frac{E_{b}}{N_{0}}\approx15~dB)$

investigate further, we ran again Algorithm 1 by considering a constant 2-path channel modeled by the CIR h = [1, -1](this is a very severe channel that happens when the two paths are in phase opposition). The obtained histograms are illustrated in Fig. 6. We observe this time that almost all Δ values of CCSK signaling are confined in the high positive region while Δ values of Hadamard signaling are distributed over the negative and the positive regions. We believe that these somewhat surprising results are due to the randomness of CCSK sequences compared to Hadamard sequences. In fact, the minimum Euclidian distance of CCSK sequences convolved with the channel is almost equal to 14.42 while it is almost equal to 2.82 for Hadamard sequences (which means that after being convolved with the channel, there are more similarities among Hadamard sequences than among CCSK sequences).

As a conclusion, CCSK signaling gives more robustness to non binary codes than Hadamard signaling in SC transmission

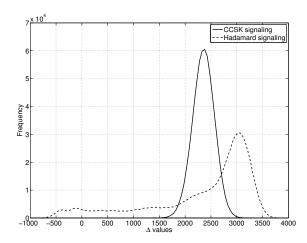


Fig. 6. Histograms of Δ for CCSK and Hadamard signaling over a constant 2-path channel in phase opposition $(\frac{E_b}{N_0}\approx 15~dB)$

with severe multipath environment. Finally, one should note that the above observations are no longer true in the case of OFDM because we transmit IFFT symbols (which introduces the same randomness to CCSK and Hadamard transmitted signals).

IV. CONCLUSION

In this paper, we investigated the performance of SC-FDE systems using NB-LDPC coded CCSK signaling. We showed that the complexity of the receiver is reduced since both LLR calculations and FDE can be simultaneously performed using a single FFT/IFFT block. Furthermore, simulations over Channel Model A demonstrated the benefits of such transmission scheme. First, NB-LDPC coded CCSK has similar performance in both SC-FDE and OFDM systems. Second, the randomness and the cyclic property of CCSK sequences make it a more attractive choice than OM for SC-FDE systems. Finally, NB-LDPC coded CCSK shows significantly better performance than binary LDPC coded CDMA. The complexity of NB-LDPC decoders is no longer a barrier since many low complexity decoding algorithms, such as the EMS algorithm, have been proposed in the literature. These features may be attractive for several future industrial applications such as sensor networks, satellite communications or acoustic communications (oil drilling, underwater communications).

V. 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.

REFERENCES

- 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.
- 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] O. Abassi, L. Conde-Canencia, M. Mansour, and E. Boutillon, "Non-Binary Low-Density Parity-Check coded cyclic Code-Shift keying," in 2013 IEEE Wireless Communications and Networking Conference (WCNC): PHY (IEEE WCNC 2013 PHY), Shanghai, P.R. China, Apr. 2013, pp. 2544–2548.
- [6] D. T. Tran, T. P. Nguyen, and X. N. Tran, "An effective frequency domain equalization scheme for cyclic prefix assisted cyclic code shift keying systems," in *Advanced Technologies for Communications (ATC)*, 2012 International Conference on, 2012, pp. 41–45.
- [7] E. Boutillon, O. Abassi, and L. Conde-Canencia, "Procédé de transmission de mots de code correcteur d'erreur non binaire avec modulation CCSK, signal et dispositif correspondant," France Patent Request 1 251 334, 02 13, 2012. [Online]. Available: http://hal.archivesouvertes.fr/hal-00758805
- [8] M. Davey and D. J. C. MacKay, "Low density parity check codes over \$\mathscr{G}\mathbb{F}(q)\]," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.
- [9] Design and versatile implementation of non-binary wireless communications based on innovative ldpc codes. [Online]. Available:

- http://www.ict-davinci-codes.eu/
- [10] D. Falconer, S. Ariyavisitakul, A. Benyamin-Seeyar, and B. Eidson, "Frequency domain equalization for single-carrier broadband wireless systems," *Communications Magazine*, *IEEE*, vol. 40, no. 4, pp. 58–66, 2002.
- [11] T. Krauss, M. Zoltowski, and G. Leus, "Simple mmse equalizers for cdma downlink to restore chip sequence: comparison to zero-forcing and rake," in *Acoustics, Speech, and Signal Processing, 2000. ICASSP* '00. Proceedings. 2000 IEEE International Conference on, vol. 5, 2000, pp. 2865 –2868 vol.5.
- [12] J. Medbo and P. Schramm, "Channel models for hiperlan/2," ETSI/BRAN doc. No. 3ER1085B, 1998.
- [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] 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.
- [15] R. Craigen and H. Kharaghani, "Hadamard matrices and hadamard designs," in *Handbook of Combinatorial Designs*, 2nd ed., C. J. Colbourn and J. H. Dinitz, Eds. Chapman & Hall/CRC, 2007.
- [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.