Generalized low-density codes with BCH constituents for full-diversity near-outage performance

Joseph J. Boutros*, Gilles Zémor†, Albert Guillén i Fàbregas‡ and Ezio Biglieri§
*Texas A&M University at Qatar, Doha, Qatar
†Institut de Mathématiques de Bordeaux, France
‡University of Cambridge, UK
§Universitat Pompeu Fabra, Barcelona, Spain

***Abstract*— A new graph-based construction of generalized low density codes (GLD-Tanner) with binary BCH constituents is described. The proposed family of GLD codes is optimal on block erasure channels and quasi-optimal on block fading channels. Optimality is considered in the outage probability sense. A classical GLD code for ergodic channels (e.g., the AWGN channel, the i.i.d. Rayleigh fading channel, and the i.i.d. binary erasure channel) is built by connecting bitnodes and subcode nodes via a unique random edge permutation. In the proposed construction of full-diversity GLD codes (referred to as root GLD), bitnodes are divided into 4 classes, subcodes are divided into 2 classes, and finally both sides of the Tanner graph are linked via 4 random edge permutations. The study focuses on non-ergodic channels with two states and can be easily extended to channels with 3 states or more.**

I. Introduction

Many researchers would admit that the problem of building powerful error-correcting codes has been in some sense solved. The adjective “powerful” refers to the capability of the channel code to achieve near Shannon capacity error rate performance. Indeed, most of those powerful codes have been constructed and analyzed in roughly one decade, between 1993 and 2004, including turbo codes, low-density parity-check codes (LDPC), raptor codes, multi-edge type codes, etc.

Nevertheless, research on analyzing and understanding the behavior of powerful graph codes on less classical channels is still under progress. What about non-ergodic channels with null Shannon capacity like block fading channels and block erasure channels encountered in wireless data transmissions such as WiFi and WiMax ? If not well designed, powerful graph codes may show a poor performance in presence of non-ergodicity, they even fail to achieve the first necessary criterion which is capturing the maximum diversity order embedded in the transmission channel [9].

In this paper, we propose to design generalized low-density (GLD) codes for non-ergodic erasure and fading channels. GLD codes are Tanner structures [1] with random permutations. The reader can find a detailed description of GLD codes in [2][3][4][5]. We are aware that practical applications and standards are mainly selecting Turbo or LDPC codes for channel coding. The aim of this paper is essentialy theoretical, we do not claim that GLD codes may compete with Turbo/LDPC codes which are very well understood and implemented by engineers. Our study of full-diversity GLD codes is motivated by

- The GLD family constitue a bridge between the classical algebraic coding theory and the modern theory of error-correcting codes based on graphs and iterative algorithms.
- GLD codes are asymptotically good, with smaller bitnode degrees when compared to LDPC .
- Minimum Hamming distance: the Gilbert-Varshamov bound is attained for different GLD families (see Fig. 3 in [3], [6]).
- ML decoding: BSC channel capacity attained for different GLD families (see Fig. 4 in [3]).
- Direct generalization of LDPC codes, replace the SPC nodes by BCH nodes.
- Direct generalization of product codes, replace the complete graph by a low density graph.
- Perform as well as Turbo and LDPC codes on non-ergodic fading channels! see the word error rate performance in the last section of this paper.

The constituent of a GLD code can be any linear block code. Due to its flexibility in terms of rate and length, the BCH family [10][11] is the best suited for defining subcode nodes in a GLD code. Even more advantages can be listed:

- The GLD coding rate R is flexible (independent from the code length), $R = 2r - 1$ for a rate-r BCH constituent when all bitnodes have degree 2. The code length is $N = Ln$, where L is a degree of freedom (compare to $N = n^2$ in product codes).
- Asymptotic analysis of GLD codes is possible, $L \to +\infty$ while R is fixed. This analysis can be made using standard tools such as Density Evolution (DE) [7].
- Irregularity can be introduced via $\lambda(x)$ in order to improve the ergodic decoding threshold and to insure an overall rate as close as possible to $1/2$.

Due to the lack of space in this paper, we dot not describe

[1] The work of Ezio Biglieri was supported by the STREP project ’DA VINCI’ within the 7th FP of the European Commission.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

the properties of block-fading channels. The reader can refer to [8], [9], and references cited therein for more information. For the same reasons, proofs of propositions stated in this paper are not given. A brief description of the channel model is given in the next section.

II. Channel model

Linear binary coding for non-ergodic channels is considered. The channel state is assumed to be invariant for some time period, finite or infinite. Given the channel state α, an input $x = \pm 1$ and an output $y = \alpha x + \eta$, the channel transition probability is

$$p(y|x, \alpha) \propto \exp\left(-\frac{|y-\alpha x|^2}{2\sigma^2}\right), \qquad (1)$$

where σ^2 is the variance of the additive white Gaussian noise η. Two cases are considered:

1) The non-ergodic Rayleigh fading channel where the fading coefficient α belongs to $\mathbb{R}^+$, with probability density function $2\alpha e^{-\alpha^2}$. We should emphasize that the root GLD codes that we introduce below achieve maximal diversity for this channel and also in presence of other types of fading distribution, as in coding for MIMO channels where a channel state is assigned a high order Nakagami distribution.
2) The block erasure channel where the fading coefficient α belongs to $\{0, +\infty\}$.

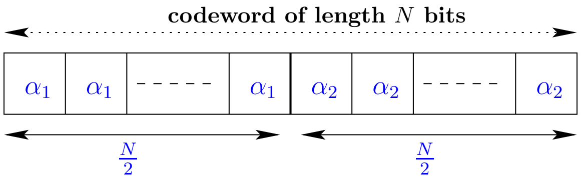

Fig. 1. Data transmission channel with 2 states.

Within a codeword of length N bits, it is assumed that α takes n_c independent values. Also, the fading instances are supposed to be independent from one codeword to another. For simplicity, we consider the case $n_c = 2$ channel states per codeword, as illustrated in Figure 1. Code construction and analysis is generally straightforward for $n_c \geq 3$. Channel coding is made via a rate-R GLD code $C[N, K]$. The code C is built from a rate-r constituent $C_0[n, k]$, also referred to as a subcode of the GLD code. In our practical examples, we are mainly focusing on subcodes defined from the famous family of linear binary BCH codes [10][11]. The next section briefly describes the structure of a GLD code.

III. Generalized low density codes with binary BCH constituents

The simplest way to introduce a GLD code is to modify the constraints in a Gallager LDPC code [12][13]. Indeed, the bipartite graph representation is identical, the single-parity checknodes in an LDPC code are replaced by BCH checknodes. The structure of the GLD parity-check matrix can be derived from the graph representation [2][4]. A different way for defining GLD codes is to modify the complete graph of a product code. Replacing the product code graph by a low-density pseudo-random graph yields a GLD code. Finally, a third equivalent method is to define a GLD code as the intersection of interleaved block codes [3]. In presence of quasi-static fading (non-ergodic channels), the information theoretical limit is given by the outage probability [14][15]. Two necessary conditions must be satisfied in order to design a near-outage achieving GLD code [16][9]:

1) In the fading plane [16], the outage boundary curve of the code must be as close as possible to the capacity outage curve on the ergodic line ($\alpha_1 = \alpha_2$). Hence, the GLD code must exhibit a low decoding threshold on ergodic channels (this is referred to as a capacity-achieving code in coding theory). Hence, we briefly describe in this section how to improve the ergodic decoding threshold with respect to regular GLD codes as originally proposed in the cited literature.
2) In the fading plane, the outage boundary curve of the code must be as close as possible to the capacity outage curve along both fading axes. This condition is equivalent to designing a full-diversity code in presence of block erasures ($\alpha_1 = 0$ and $\alpha_2 = +\infty$, and vice versa). The construction of a full-diversity code is given in the next section.

Let us consider a GLD code with an irregular bitnode degree distribution defined by a sequence $\{\lambda_i\}$. For simplicity, the subcode nodes are all identical (the GLD is right regular). Let d denote the highest bitnode degree. Recall that all subcode nodes have degree n. The degree distribution satisfies the following constraints:

$$0 \leq \lambda_i \leq 1, \quad \sum_{i=1}^{d} \lambda_i = 1, \quad \sum_{i=1}^{d} \frac{\lambda_i}{i} = \frac{1-r}{1-R}, \qquad (2)$$

where $r = k/n$ and $R = K/N$. It is assumed that the graph constraints are all independent. If the degree distribution is restriced to $\{1, 2, d\}$, then the overall GLD rate is

$$R = 1 - \frac{2(1-r)}{1 + \lambda_1 - (1 - \frac{2}{d}\lambda_d)}, \qquad d \geq 3. \qquad (3)$$

Improving the ergodic threshold of GLD codes. Instead of restricting the GLD structure to $\lambda_2 = 1$, a slight improvement in the decoding threshold can be obtained by introducing λ_1 and λ_d, where $d \geq 3$. Despite the small improvement on an ergodic Gaussian channel, the move on the ergodic line is sufficient to produce near-outage performance as shown in the last section. The fraction λ_1 is also useful to increase the coding rate up to $1/2$ (the highest rate according to the block-fading Singleton bound). The number of bitnodes of degree 1 should be limited within a subcode node as stated below.

Proposition 1: Let $C[N, K]$ be a GLD code built from a constituent $C_0[n, k, d_{min}]$ with an irregular bitnode degree distribution. Let λ_1 be the fraction of edges connected to mono-edge bitnodes. Let μ be the maximum number of mono-edge bitnodes connected to a subcode node. In order to avoid error-floors under iterative decoding, μ must satisfy

$$\mu \leq d_{min} - 2 \tag{4}$$

Hence, the fraction λ_1 is upper bounded as follows

$$\lambda_1 \leq \frac{\mu}{n} \leq \frac{d_{min} - 2}{n} \tag{5}$$

The ratio of λ_1 to its maximal value is

$$\lambda_{11} = \frac{\lambda_1}{(\mu/n)} \tag{6}$$

We also define the polynomial $\lambda(x)$ (not including λ_1) for use in density evolution [13],

$$\lambda(x) = \frac{\sum_{i\geq 2} \lambda_i x^{i-1}}{\sum_{i\geq 2} \lambda_i} \tag{7}$$

Let $f^m(x)$ denote the probability density function of log-ratio messages propagating from bitnodes to subcode nodes at iteration m. The standard convolution is denoted by $\otimes$. The BCH probabilistic decoder is denoted by Φ. The superscript $\odot$ represents the number of inputs. For example, the notation $\Phi\left[f^m(x)^{\odot n-1}\right]$ represents the probability density function of extrinsic log-ratio messages at the BCH decoder output when the density $f^m(x)$ is applied at its $n-1$ inputs. Let $\mu(x)$ be the gaussian density at the output of the AWGN channel without fading ($\alpha_1 = \alpha_2 = 1$). The following proposition establishes the expression of density evolution for GLD codes on AWGN memoryless channels (without fading) with BPSK input.

Proposition 2: The density of log-ratio messages propagating from bitnodes to subcode nodes for an irregular GLD code satisfies

$$f^{m+1}(x) = \mu(x) \otimes \lambda\left(\Phi[u, v]\right) \tag{8}$$

with $u = f^m(x)^{\odot n-\mu-1}$ and

$$v = \left(\lambda_{11}\mu(x) + (1 - \lambda_{11})f^m(x)\right)^{\odot\mu}$$

where $f^0(x) = \mu(x)$, λ_{11} is given by (6), $\lambda(x)$ is defined in (7), and m is the decoding iteration number.

Consider the GLD code built from $C_0[15, 11, 3]$. When $\lambda_2 = 1$, the overall rate is $R = 0.46666$ and the ergodic threshold is $E_b/N_0(min) = 0.84dB$ on AWGN channel with BPSK input. The irregular version based on $C_0[15, 11, 3]$ with $\lambda_1 = 0.660000$, $\lambda_2 = 0.912122$, and $\lambda_4 = 0.021878$ have $R = 0.4945$ and $E_b/N_0(min) = 0.73dB$.

IV. Full-Diversity GLD Codes based on Root Subcodes

A rootcheck is a special type of checknode suitable for designing codes on graphs matched to iterative decoding when transmitted over block-fading and block-erasure channels.

Definition 3: A type 1 rootcheck is a subcode node that recovers all the values of the incident bit nodes when a block erasure occurs on channel 1. It will be convenient to call the incident bit nodes that are transmitted on channel 1 *rootnodes* and all the other incident bits *leafbits* (or leaves). Note that all leafnodes of a type 1 rootcheck are transmitted on channel 2. A type 2 rootcheck is defined similarly by interchanging the roles of channels 1 and 2.

The definition of a rootcheck is illustrated by Figure 2 below, where all roots are colored in white and all leaves colored in red.

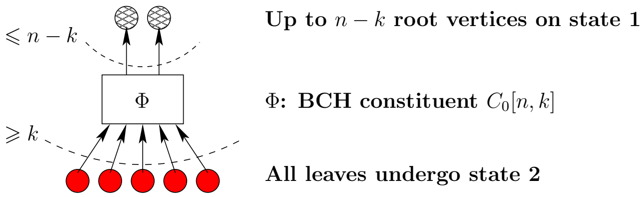
$\leqslant n-k$
Up to $n-k$ root vertices on state 1
Φ
Φ: BCH constituent $C_0[n,k]$
$\geqslant k$
All leaves undergo state 2

Fig. 2. Structure of a rootcheck for a 2-state channel. All root bits are transmitted on fading 1 (white) and all leaves on fading 2 (red). A dual rootcheck is defined by interchanging the two fading numbers.

The version of the constituent C_0 defined by a parity-check matrix H_0 and used in a rootcheck must satisfy the following constraint:

The $n-k$ root vertices are assigned to $n-k$ independent columns of H_0. The simplest convention is to write the parity-check matrix in systematic form, $H_0 = [I_{n-k} \mid P_0]$, and assign the first $n-k$ columns to root bitnodes. As shown in Fig. 2, if root bits are erased then one can recompute their value from leaf bits using H_0.

Proposition 4: A rootcheck $C_0[n, k, d]$ guarantees full diversity to all its roots under both block erasures and block fadings.

Using the rootcheck as a building block, the Tanner graph of a full-diversity GLD code can be derived directly from the representation of product codes or that of LDPC codes. Both prodecures lead to the same bipartite Tanner graph (details omitted) depicted in Fig. 3.

Bitnodes are divided into 4 classes. Nodes 1i are information bits transmitted on state 1, nodes 2i are information bits transmitted on state 2. All information bits are protected by rootchecks (rootchecks 1c for bits 1i and rootchecks 2c for bits 2i). Parity bits are denoted 1p and 2p. Diversity is not guaranteed on parity bits because they are not rootbits. The reader can easily check on Fig. 3 how bitnodes 1i can be determined in 1 iteration if all white bits are erased (i.e., erase both 1i and 1p). Numbers on the left and on the right represent the cardinality of each node family. For example, the root GLD has $RN/2$ bits of type 1i and $(1-R)N/2$ bits of type 2i. The code has also N/n subcode nodes for types 1c and 2c. The parity-check matrix of C can be directly derived from its Tanner graph. An example is shown in Fig. 4 for $R = 1/2$.

In contrast to classical fully random GLD codes, a root GLD is built via 4 random edge permutations, $1i \leftrightarrow 2c$, $1p \leftrightarrow 2c$, $2p \leftrightarrow 1c$, and $2i \leftrightarrow 1c$. Therefore, root GLD codes are generalized multi-edge type low-density codes [17] suited for

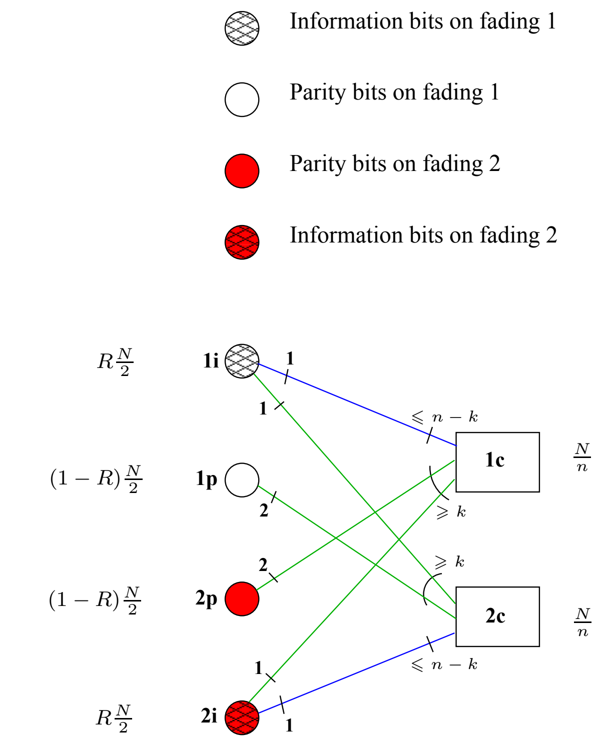

Fig. 3. Tanner graph of a full-diversity regular GLD code (root GLD) to be transmitted on a 2-state non-ergodic fading channel, rate $R \leq 1/2$ and length N.

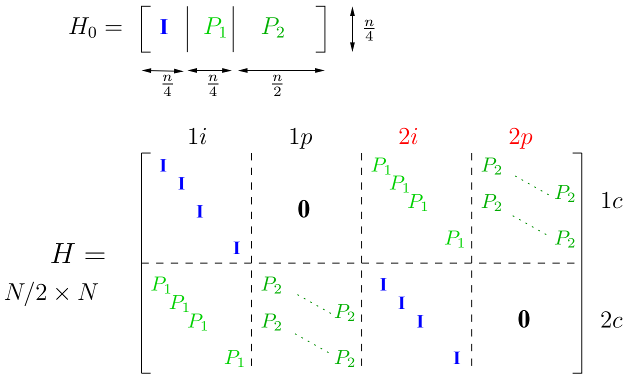

Fig. 4. Parity-check matrix for a regular root GLD, $r = 3/4$ and $R = 1/2$. Column permutations are not shown.

iterative decoding over block-fading channels. Irregular degree distribution $\{\lambda_i\}$ can be easily embedded in the Tanner graph of a root GLD. In order to maintain full diversity, mono-edge bitnodes connected to 1c belong to 1i and 2p only. Similarly, mono-edge bitnodes connected to 2c checks belong to 2i and 1p. Bitnodes of degree 2 and more can be spread over the 4 classes without any restriction (except for perfect symmetry that must be satisfied when interchanging fading numbers 1 and 2).

The final proposition stated below establishes the density evolution of a full-diversity root GLD code on a 2-state block-fading channel. Density evolution is not as standard as usually expected when dealing with full-diversity root-GLD codes. Different types of messages will be propagating in the code (4 pdfs when $n_c = 2$ channel states). Let us define the following sums,

$$S_1 = \sum_{i \geq 2} \frac{\lambda_i}{i} \qquad S_2 = \sum_{i \geq 2} \frac{\lambda_i}{i-1} \qquad S_3 = \sum_{i \geq 1} \frac{\lambda_i}{i}, \tag{9}$$

and the following multi-edge fractions

$$f_{e1} = 1 - g_{e1} = \frac{RS_1}{(1-R)S_2 + RS_1} \tag{10}$$

$$f_{e2} = 1 - g_{e2} = \frac{R}{R + (1-R)/S_3 - 2r + R/S_2} \tag{11}$$

Using the same notation for log-ratio messages as in section V of [9], mainly,

- $\mu_1(x)$: the gaussian density at the output of the channel with fading α_1. Similarly, $\mu_2(x)$ is the pdf at the channel output when fading is α_2. The all-zero codeword is assumed to be transmitted [7].
- $q_1^m(x)$ and $q_2^m(x)$: Probability density functions of log-ratio messages on the edges $1i \rightarrow 1c$ and $2i \rightarrow 2c$ respectively.
- $f_1^m(x)$ and $f_2^m(x)$: Probability density functions of log-ratio messages on the edges $1i \rightarrow 2c$ and $2i \rightarrow 1c$ respectively.

Let us define the density mixtures

$$\begin{aligned} \mu_{12}(x) &= f_{e2}\mu_1(x) + g_{e2}\mu_2(x) && (12)\\ \mu_{21}(x) &= f_{e2}\mu_2(x) + g_{e2}\mu_1(x) && (13)\\ q_{12}(x) &= f_{e2}q_1(x) + g_{e2}q_2(x) && (14)\\ q_{21}(x) &= f_{e2}q_2(x) + g_{e2}q_1(x) && (15) \end{aligned}$$

Now, the final proposition can be stated.

Proposition 5: At iteration $m+1$, for a fixed fading pair (α_1, α_2), density evolution equations of a root GLD code on a block-fading channel are

$$\begin{aligned} f_1^{m+1}(x) &= \mu_1(x) \otimes \phi_{11}(x) \otimes \tilde{\lambda}(\phi_{21}(x)) \\ q_1^{m+1}(x) &= \mu_1(x) \otimes \lambda(\phi_{21}(x)) \end{aligned}$$

where $\tilde{\lambda}(x) = \lambda(x)/x$. The extrinsic densities $\phi_{11}(x)$ (from 1c to 1i) and $\phi_{21}(x)$ (from 2c to 1i) are given by $\phi_{11}(x) = \Phi_{n-k-\mu}[u, v, w]$ with

$$\begin{aligned} u &= [f_{e1}f_2(x) + g_{e1}q_2(x)]^{\odot k} \\ v &= [q_{12}(x)]^{\odot n-k-\mu-1} \\ w &= [\lambda_{11}\mu_{12}(x) + (1-\lambda_{11})q_{12}(x)]^{\odot \mu} \end{aligned}$$

and $\phi_{21}(x) = \Phi_k[u, v, w]$ with

$$\begin{aligned} u &= [f_{e1}f_1(x) + g_{e1}q_1(x)]^{\odot k-1} \\ v &= [q_{21}(x)]^{\odot n-k-\mu} \\ w &= [\lambda_{11}\mu_{21}(x) + (1-\lambda_{11})q_{21}(x)]^{\odot \mu} \end{aligned}$$

Similar equations are obtained by permuting the two fading numbers. The index m is omitted from ϕ_{11} and ϕ_{21} to simplify the expressions.

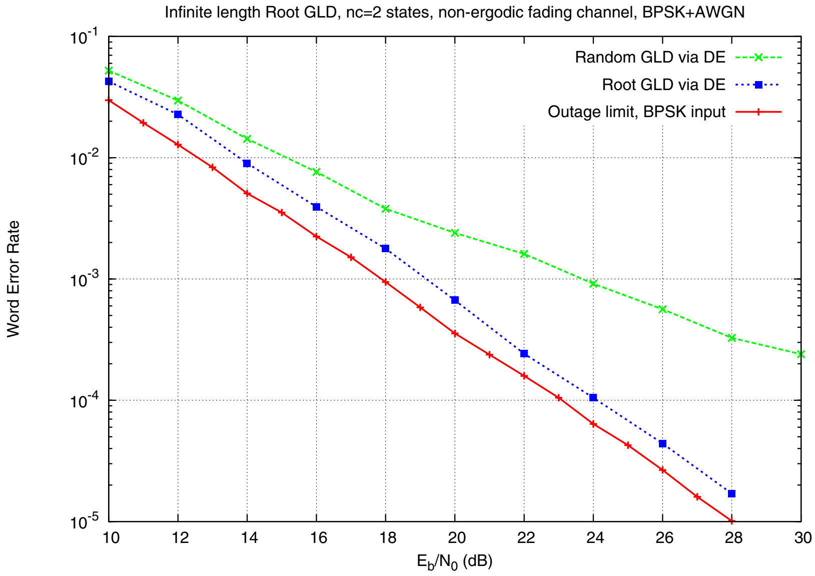

Fig. 5. Performance of random and root GLD (infinite length via DE) on a Rayleigh block-fading channel, $n_c = 2$ states.

V. Numerical Results

The word error rate performance versus signal-to-noise ratio per bit is plotted in Fig. 5 for a GLD code based on $C_0[15, 11]$, with degree distribution $\{\lambda_i\}$ given at the end of section III, i.e., $\lambda_1 = 0.66$ and $R = 0.4945$. For the same degree distribution, the performance of random and root GLD codes is determined via density evolution as given in proposition 5. As expected, a random Tanner graph cannot guarantee the full diversity order (diversity is 1), its error rate decreases as $1/(E_b/N_0)$. The root structure based on rootchecks has an error rate decreasing as $1/(E_b/N_0)^2$ (diversity is 2) with a performance relatively close to the information theoretical limit given by the outage probability for 0.4945 bits per channel use.

References

[1] R.M. Tanner, “A recursive approach to low complexity codes,” *IEEE Trans. on Inf. Theory*, vol. IT-27, no. 5, pp. 533-547, Sept 1981.

[2] O. Pothier, “Compound codes based on graphs and their iterative decoding,” *PhD thesis in communications and electronics, ENST*, Paris, Jan. 2000. Click to download.

[3] O. Pothier, L. Brunel, and J.J. Boutros, “A low complexity FEC scheme based on the intersection of interleaved block codes,” *IEEE Vehicular Technology Conference*, vol. 1, pp. 274-278, Houston, USA, May 1999. Click to download.

[4] J.J. Boutros, O. Pothier, and G. Zémor, “Generalized low density (Tanner) codes,” *IEEE International Conference on Communications*, vol. 1, pp. 441-445, Vancouver, Canada, June 1999. Click to download.

[5] M. Lentmaier and K.S. Zigangirov, “On generalized low-density parity-check codes based on Hamming component codes,” *IEEE Comm. Letters*, vol. 3, no. 8, Aug. 1999.

[6] A. Barg and G. Zémor, “Distance properties of expander codes”, *IEEE Trans. on Information Theory*, IT-52, No 1 (2006) pp. 78–90.

[7] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2007.

[8] D.N.C. Tse and P. Viswanath, *Fundamentals of Wireless Communications*, Cambridge University Press, 2005.

[9] J.J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zémor, “Low-density parity-check codes for nonergodic block-fading channels,” *Submitted to the IEEE Trans. on Inf. Theory*, Oct 2007. Click to download.

[10] R.E. Blahut, *Algebraic codes for data transmission*. Cambridge University Press, 2003.

[11] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, eight impression (1991), North-Holland, 1977.

[12] R.G. Gallager, Low-density parity-check codes, MIT Press, 1963.

[13] T.J. Richardson and R.L. Urbanke, “The capacity of low-density parity-check codes under message-passing decoding,” *IEEE Trans. on Inf. Theory*, vol. 47, no. 2, pp. 599-618, February 2001.

[14] L.H. Ozarow, S. Shamai (Shitz), and A.D. Wyner, “Information theoretic considerations for cellular mobile radio,” *IEEE Trans. on Vehicular Tech.*, vol. 43, no. 2, pp. 359-378, May 1994.

[15] E. Biglieri, J. Proakis, and S. Shamai (Shitz), “Fading channels: Information-theoretical and Communications aspects,” *IEEE Trans. on Inf. Theory*, vol. 44, no. 6, pp. 2619-2692, Oct. 1998.

[16] J.J. Boutros, A. Guillén i Fàbregas, and E. Calvanese Strinati, “Analysis of coding on non-ergodic channels,” *Allerton’s Conference*, Monticello, Illinois, Sept 2005. Click to download.

[17] T. J. Richardson and R. L. Urbanke, “Multi-edge type LDPC codes,” *IEEE Trans. on Inf. Theory*, to appear. Click to download.