Full-diversity Product Codes for Block Erasure and Block Fading Channels

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

***Abstract*— We show how to build full-diversity product codes under both iterative encoding and decoding over non-ergodic channels, in presence of block erasure and block fading. The concept of a rootcheck or a root subcode is introduced by generalizing the same principle recently invented for low-density parity-check codes. We also describe some channel related graphical properties of the new family of product codes, a family referred to as root product codes.**

I. Introduction

Product codes are powerful compound codes with rich and elegant graphical and algebraic structures. Their error and erasure correcting capabilities in both bursty and non-bursty modes have been extensively studied in the two decades following their invention by Elias [8]. One of the simplest methods for combining two codes is to form their direct product, see [13], Chap. 18. Besides its nice algebraic properties [4][12][13], a product code has a graphical representation that can lead to even more powerful generalizations under both iterative encoding and decoding [20]. The interest in product codes has been propelled by their excellent performance under iterative decoding on classical ergodic Gaussian channels [16]. Several studies have been carried out on decoding product codes [1][9][15], analyzing their asymptotic and low error rate performance [7][17][18], unveiling more properties of their weight distribution [21], proposing design criteria and analyzing their erasure rate in the presence of ergodic i.i.d erasures [2][22], and describing the convergence of their iterative decoding [19].

In this paper, erasures and fadings encountered during transmission are not independent from one binary digit to another, they occur in blocks and are constant within a block, see e.g. [3], Chap. 4. The exact channel model will be given in section III. Given a data transmission channel with n_c internal states, where n_c is referred to as the channel diversity order, an error-correcting code achieves a d-diversity order after decoding, e.g. on a BSC channel with transition probability p, when the error rate at the decoder output can be written in the form $P_e \propto p^d$. The code is *full diversity* if $d = n_c$. In the absence of unit-rate linear precoding before transmission [10] (e.g. a unitary transformation), the *block fading Singleton bound* [11], [14] states that $d \leq \lfloor n_c(1 - R_c) \rfloor + 1$ for a rate R_c code. A code achieving the Singleton bound is said to be *maximum distance separable* (MDS). An MDS code is not necessarily full diversity, but a full-diversity code is necessarily MDS with coding rate $R_c \leq 1/n_c$.

Properties and methods for designing full-diversity product codes are studied in this paper. Our study is restricted to bi-dimensional binary product codes. Some similarities exist between our product codes and array codes such as the dual of B-codes [23]. Both families are MDS, but array codes are not full-diversity and they are designed for channels with a relatively large diversity ($n_c = 5, 6$ or more) while our codes are meant for channels with limited diversity (n_c =2 or 3). We start with a small example that summarizes the design problem and the principal ideas.

II. Problem Illustration

We illustrate the problem studied in this paper by setting block erasures on a simple product code. Consider the product code C of the single parity codes of lengths 3 and 4. The code C can be viewed as the set of 3×4-matrices whose rows and columns are all of even weight : it is of length 12, dimension 6 (rate $R = 1/2$). Note that for complexity reasons, we only allow ourselves row and column operations both for encoding and for decoding.

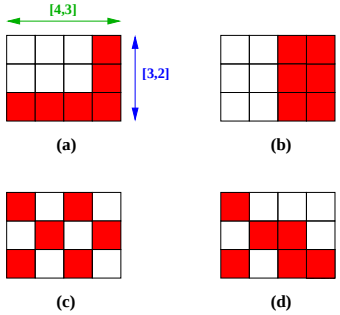

Fig. 1. Four different channel interleaving of code symbols. In the context of non-ergodic channels, the 4 configurations define 4 different product codes.

The matrix structure of codewords of C is shown on Figure 1. Half the boxes (bit positions) are colored in white and the other half in red. Assume all bits of one color are erased. Is the code C capable of finding them with only the residual color ?

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

Four different colorings of the product code are given in Figure 1. In practice, they are equivalent to four different channel interleavers (also known as multiplexers) applied on code symbols. Consider the product code defined by Figure 1(a). If all red bits are erased, the decoding of the first two rows followed by the decoding of the 4 columns will fill the erasures. Unfortunately, if white bits are all erased, any number of row-column decoding iterations will never retrieve the erased values. Hence, in the terminology of communication theory, we would say that code 1(a) is not full diversity. The reader can check that 1(b) and 1(c) are not full-diversity codes.

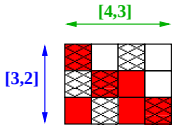

Fig. 2. The full-diversity product code defined in Figure 1(d). Privileged bits are indicated by a pattern.

The product code defined in Figure 1(d) is full diversity. Indeed, if all red bits (similarly if all white bits) are erased, the decoder is capable of filling their values after 3 decoding iterations (row $\rightarrow$ column $\rightarrow$ row). The first bit (in red) on the first row is privileged because all other bits belonging to the same row are of the opposite color. A privileged bit, if erased, can be recovered in one decoding iteration. Figure 2 depicts code 1(d) with privileged bits indicated by a pattern. Those bits are said to be connected to a *rootcheck*.

The standard location of information bits is the upper left 2×3 corner. The position of information bits can be moved to those connected to rootchecks. The new full-diversity code is referred to as a root product code. It has the following properties:

- It is full diversity on both block erasure and block fading channels.
- Full diversity is achieved after one decoding iteration. Indeed, erased information bits are recovered in one decoding iteration (two iterations if we account for row and column decoding, since some bits are recovered via their horizontal rootcheck, others via their vertical rootcheck).
- Its rate meets the block fading Singleton bound.

What about larger product codes, for example can we build a root product code $[16, 11]^{\otimes 2}$? If all symmetries are taken into account, the number of configurations to examine exhaustively is about 2^{160}. We will use the rootcheck concept to design full-diversity product codes

III. Channel Model and Notation

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

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

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 maximal diversity is still achieved in presence of other types of fading distribution, as in coding for MIMO channels [6] where a channel state is assigned a high order Nakagami distribution.
2) The block erasure channel where the fading coefficient α belongs to $\{0, +\infty\}$.

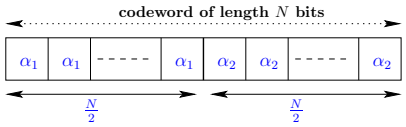

Fig. 3. Data transmission channel with 2 states.

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 3. Code construction and analysis is generally straightforward for $n_c \geq 3$. Channel coding is made via a rate-R product 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 product code. Thus, we have $C = C_0 \otimes C_0$, $N = n^2$, $K = k^2$, and $R = r^2$.

The channel diversity order is given by the number of independent channel states. The Tx/Rx diversity order, controlled by the system designer on the transmit and receive sides, is the number of independent replicas of the same information. At high signal-to-noise ratio $\gamma = \frac{1}{\sigma^2} \gg 1$, on a block fading channel of diversity order $d = n_c$, the word error rate behavior should be

$$P_e \propto \gamma^{-d}. \tag{1}$$

On a block erasure channel of diversity order $d = n_c$, for a given block erasure probability equal to ϵ, the word error rate behavior should be

$$P_e = \epsilon^d. \tag{2}$$

An error-correcting code whose error rate satisfies (1) and (2) after decoding is a full-diversity channel code. According to the block fading Singleton bound, the coding rate R of a full-diversity code is upper-bounded by:

$$R_{max} = \frac{1}{n_c} \geq R. \tag{3}$$

The two following propositions are essential in the design of coding for non-ergodic channels. Their proofs are simple and are left to the reader. For any code structure, under

ML decoding, full diversity on block erasure channels is a necessary condition for full diversity on non-ergodic Rayleigh fading channels. This can be stated as follows

Proposition 1: Consider a linear binary code $C[N,K]$. If C is full diversity on a block erasure channel then it is full diversity on a block fading channel under ML decoding.

As described in the next section, the special root structure for any compound code achieves full diversity under iterative decoding. In this paper, we are concerned with product codes only. Other full-diversity codes such as Turbo, LDPC, and GLD/Tanner codes have been constructed by the authors, see [5] and references therein.

Proposition 2: Consider a linear binary code $C[N,K]$ with a root structure (LDPC, Product, GLD, etc). Under iterative decoding, the code is full diversity on both block erasure and block Rayleigh fading channels.

IV. Root Checknodes for Linear Codes

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. In Tanner's terminology [20], the constituent of a product code will also be called a *subcode*, or a *subcode node*. In our practical examples, we mainly focus on subcodes defined from the famous family of linear binary BCH codes [4][13].

Definition 3: A rootcheck is a subcode node with all roots colored in one color and all leaves colored in the opposite color.

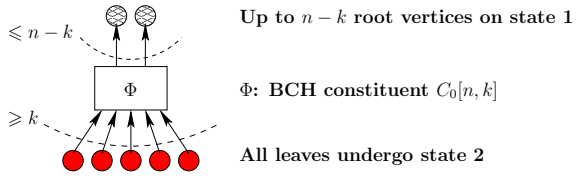

Fig. 4. Structure of a rootcheck for a 2-state channel.

The definition of a rootcheck is illustrated by Figure 4. 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. At the subcode level, we have the following equivalent of Proposition 2 for the erasure channel :

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

Proof: If root bits are erased then recompute their value from leaf bits using H_0. ∎

For the block fading channel we have :

Proposition 5: A rootcheck $C_0[n,k,d]$ guarantees full diversity to all its roots under block fading.

Proof: Local optimal probabilistic decoding is given by

$$APP(b) \propto \sum_{c \in C_0 | b} p(y|c), \tag{4}$$

where b is a root. The sub-optimal log-map decoder considers the dominant likelihoods for $b=0$ and $b=1$. Its log-ratio message is

$$\Lambda \;=\; \|y-\alpha\bar{x}\|^2 - \|y-\alpha x\|^2 \;=\; 2Y+\nu, \tag{5}$$

$$Y = \alpha_1^2 \sum_{i=1}^{n-k}(x_i-\bar{x}_i) + \alpha_2^2 \sum_{i=n-k+1}^{n}(x_i-\bar{x}_i) \;=\; \omega_1\alpha_1^2+\omega_2\alpha_2^2. \tag{6}$$

At high SNR, we have $\omega_1 \geq 1$ and $\omega_2 \geq 1$. The exact values for ω_i depend on the weight distribution of C_0. The 4th order χ^2 distribution of Y guarantees the double diversity. ∎

V. Full-Diversity Product Codes

The primary role of a full-diversity code is to ensure the highest diversity order for its information symbols. Such a protection is less important for parity-check symbols. Hence, the following definition :

Definition 6: A root product code is a product code where all *information* bits are covered by rootchecks, i.e., all information bits are rootbits belonging to a row or a column rootcheck.

From Propositions 4 & 5 and the above definition, we deduce that a root product code is full diversity under iterative decoding on both block fading and erasure channels. The maximal diversity order is reached after one decoding iteration when parallel scheduling is applied, or after two decoding iterations if serial row-column scheduling is performed.

The information rate should not be sacrificed on behalf of diversity. Thus, for $n_c = 2$, we should avoid rate $1/3$ codes which are capable of attaining a 3rd order diversity. The product code will be devised according to specific properties.

Design Property 7: The design coding rate satisfies the following inequalities:

$$\frac{1}{3} < R \leq \frac{1}{2}, \quad \text{or equivalently} \quad \frac{\sqrt{3}}{3} < r \leq \frac{\sqrt{2}}{2}.$$

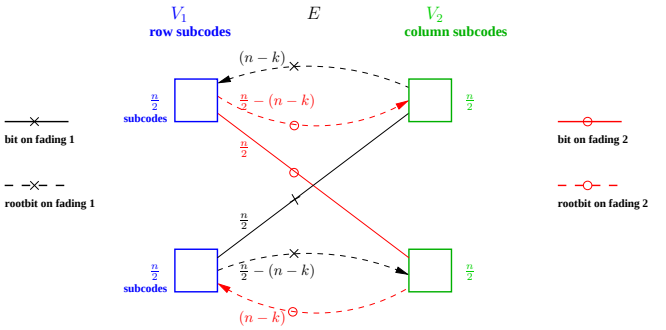

Fig. 5. Compact graph of a full-diversity product code with 2 supernodes on each side. Arrows are pointing to rootchecks of the corresponding bit. Graph notations defined in this figure will be used in the sequel. This representation is modified later in order to yield a graph-encodable product code as shown for example in Figure 6 for $r=\frac{2}{3}$.

A product code $C[N,K] = C_0[n,k]^{\otimes 2}$ is graphically represented by a complete bipartite graph (V_1,V_2,E), where V_1 is the set of row subcodes, V_2 is the set of column subcodes, and E is the set of all bits. The vertices of V_1 and V_2 are

completely connected. We also have $|V_1| = |V_2| = n$ vertices and $|E| = n^2$ edges. By convention, row subcodes are drawn on the left and column subcodes on the right. Since we are considering non-ergodic channels with 2 states, V_1 and V_2 are split into two supernodes each containing $\frac{n}{2}$ subcodes. This compact graph representation is depicted in Figure 5. Bits are associated to edges linking row subcodes to column subcodes. Arrows in Figure 5 point to rootchecks of the corresponding bits.

Let us first focus on the upper supernode of V_1. All rows have been assumed to be rootchecks, each of them containing $n-k$ roots as indicated on the edges undergoing fading α_1. Because the graph is complete, the number of edges linking a row supernode and a column supernode must be equal to $\frac{n}{2}$. Hence, there are $\frac{n}{2} - (n-k)$ bits with state α_2 linking the two upper supernodes and $\frac{n}{2}$ bits linking diagonally opposed supernodes from V_1 to V_2, as clearly indicated in Figure 5. The graph structure in the lower supernodes is symmetric to that of upper ones. The graph construction is still valid for odd n and for asymmetric product codes but it should be slightly modified accordingly.

Notice that $\frac{n}{2} - (n-k)$ is a non-negative integer since $\frac{1}{2} < \frac{\sqrt{3}}{3} < r$. Finally, the number of rootbits K_r is

$$K_r = 2 \times \frac{n}{2} \times \left((n-k) + \frac{n}{2} - (n-k) \right) \quad \geq \quad k^2 = K,$$

because $R \leq \frac{1}{2}$. We conclude that all information bits can be covered by rootchecks, i.e., the graph representation given in Figure 5 with 2 supernodes on each side represents a full-diversity product code. We may also be tempted to announce now that a simple solution has been found for the construction of full-diversity root product codes at any rate satisfying design property 7. Unfortunately, the diagonal links have $\frac{n}{2}$ digits which are parity bits of C. The constituent code C_0 cannot successfully carry out the computation of those parity bits based on the knowledge of information bits because $\frac{n}{2} > (n-k)$ as mentioned above. Therefore, iterative encoding of the product code $C = C_0 \otimes C_0$ based on its row and column subcodes C_0 is impossible when V_1 and V_2 are split into 2 supernodes. In an equivalent terminology, we say that such a structure is not graph encodable.

Design procedure. The compact graph of a graph-encodable root product code is built as follows:

- The number of edges linking two supernodes should be equal to the number of supernodes since the graph is complete.
- To render a graph-encodable code, the number of supernodes cannot be equal to 2 as in the previous graph representation. The number of non-root bits must be less than or equal to $n-k$. In order to let the rootchecks cover all constituent information bits, the number of supernodes in V_1 and V_2 should be taken equal to

$$\left\lceil \frac{n}{n-k} \right\rceil,$$

  i.e., this is the number of supernodes on each side of the compact graph representation, where a supernode does not contain more than $n-k$ subcodes.
- Colors should be selected in order to maximize the number of rootbits. After color selection, information bits are placed on root edges.

We first restrict ourselves to graphs with strong symmetries where rootbits are decoded in one shot as a consequence of Definition 3. This type of first order rootbit is to be opposed to high order rootbits as defined in the next section, where the compact graph has less symmetries. Now, we impose the following design property which is inherited from the initial graph with 2 supernodes on each side.

Design Property 8: A supernode of V_1 or V_2 has a maximum of 2 super-edges associated to rootbits, one super-edge with incoming rootbits and the other with outgoing rootbits.

A super-edge is an edge linking two supernodes in the compact graph representation. Our design procedure for first-order root product codes limits the number of binary elements within a superedge to a maximum of $n-k$ bits.

Let us assume that all rootchecks are row subcodes, then the code guarantees full diversity for all its information bits if $n(n-k) \geq k^2$, i.e. $r^2 + r - 1 \leq 0$.

Proposition 9: A full-diversity product code $C_0[n,k]^{\otimes 2}$ with all its rootchecks being row subcodes satisfies $r = \frac{k}{n} \leq \frac{\sqrt{5}-1}{2}$.

Such an unbalanced code should be avoided in practice. The constituent coding rate should be lower bounded by $(\sqrt{5}-1)/2$ instead of $\sqrt{3}/3$ as stated in the design property 7. Now, let us examine encoding on the subcode level for a non-ergodic channel with 2 states. A root product code is graph-encodable if the subcode dimension does not exceed the number of incoming and outgoing roots, i.e., if $k \leq 2(n-k)$.

Proposition 10: A graph-encodable full-diversity root product code exists if $r = \frac{k}{n} \leq \frac{2}{3}$.

From the above propositions, we conclude that a valid range for the rate of the product code constituent is

$$\frac{\sqrt{5}-1}{2} \leq r \leq \frac{2}{3}.$$

Corollary 11: A graph-encodable full-diversity root product code $[16, 11, 4]^{\otimes 2}$ does not exist.

Of course, this corollary is meant for first order root codes. A third order full-diversity $[16, 11, 4]^{\otimes 2}$ code is built in the next section. Finally, we end this section by illustrating our design procedure in Figures 6 and 7 with a square product code based on the $[12, 8]$ linear binary constituent.

VI. Product Codes with High-Order Rootchecks

We now drop the constraint that information bits should be decoded after just one iteration which implied that the number K_r of rootbits is at least k^2. By allowing more iterations we shall be able to deal with cases when $K_r < k^2$. Let us say that a rootbit has order ρ if it is recovered after ρ iterations. Since the girth in the product code graph is equal to 4, order-4 rootbits do not exist, which translates as :

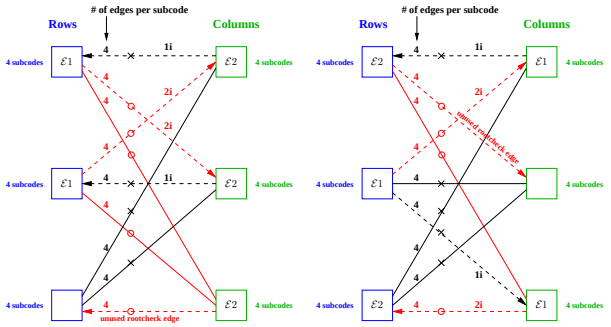

Fig. 6. Two compact graph representations of a full-diversity product code $[12,8,3]^{\otimes 2}$, $r=\frac{2}{3}$ and $R=\frac{4}{9}=0.4444$. Information bits transmitted on fading 1 (resp. fading 2) are indicated on the graph edges by $1i$ (resp. $2i$). The encoding can be made via the graph using the activation schedule $\mathcal{E}1$ followed by $\mathcal{E}2$. Any channel state (α_1 or α_2) can be assigned to unused rootcheck edges.

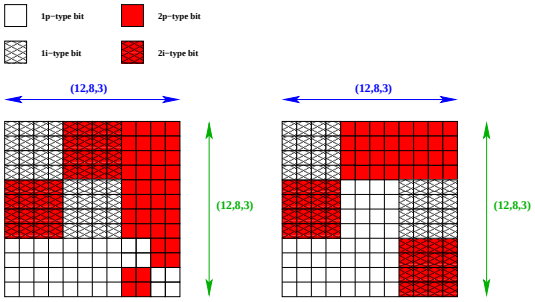

Fig. 7. Matrix representations of the full-diversity product codes $[12,8]^{\otimes 2}$ defined by the compact graphs in Figure 6.

Proposition 12: A root product code attains full diversity order (or equivalently recovers all information bits) after at most 3 decoding iterations.

An example of a full-diversity product code $[16,11]^{\otimes 2}$ together with its decoding scheme is given on Figure 8. Construction details are omitted in this extended abstract.

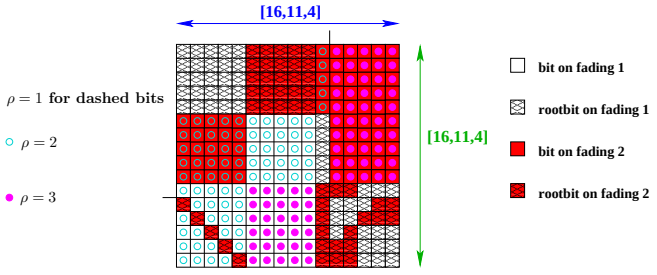

Fig. 8. Full-diversity root product code $[16,11,4]^{\otimes 2}$ of order 3. Overall coding rate is $R=0.4726$, 3 iterations are needed to attain full diversity. For a given bitnode, ρ iterations are needed to reach full diversity under parallel scheduling.

VII. Conclusions

A finite-length design of bi-dimensional binary product codes suitable for block fading channels has been proposed. The study is based on graphical tools and some simple algebraic properties of product codes. Codes at several coding rates capable of achieving the highest diversity order have been found. This work should be enhanced via the analysis of the coding gain and the general asymptotic performance behavior of product codes on non-ergodic channels.

References

[1] O. Al-Askary, "Iterative decoding of product codes," Dissertation, Royal Institute of Technology, Stockholm, April 2003.

[2] A.A. Al-Shaikhi and J. Ilow, "Erasure rate analysis and tighter upper bound for binary product codes," *IEEE Communications Letters*, vol. 10, no. 7, July 2006.

[3] E. Biglieri, Coding for Wireless Channels, Springer, May 2005.

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

[5] 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 Transactions on Information Theory*, Oct 2007. Click to download.

[6] J.J. Boutros, G.M. Kraidy, and N. Gresset, "Near outage limit space-time coding for MIMO channels," *Inaugural ITA workshop*, UCSD, San Diego, California, Feb. 2006. Click to download.

[7] F. Chiaraluce and R. Garello, "Extended Hamming product codes analytical performance evaluation for low error rate applications," *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 2353-2361, Nov. 2004.

[8] P. Elias, Error-free coding, *IRE Transactions on Information Theory*, pp. 29-37, 1954.

[9] D.F. Freeman and A.M. Michelson, "A two-dimensional product code with robust soft-decision decoding," *IEEE Transactions on Communications*, vol. 44, no. 10, pp. 1222-1226, Oct. 1996.

[10] N. Gresset, J.J. Boutros, and L. Brunel, "Optimal linear precoding for BICM over MIMO channels," *IEEE International Symposium on Information Theory*, pp. 66, Chicago, Illinois, June 2004.

[11] R. Knopp and P.A. Humblet,"On coding for block fading channels," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 189-205, Jan. 2000.

[12] F.R. Kschischang, Product Codes, J.G. Proakis (ed), *Wiley Encyclopedia of Telecommunications*, New York, 2003.

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

[14] E. Malkamaki and H. Leib, "Evaluating the performance of convolutional codes over block fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1643-1646, Jul. 1999.

[15] S.A. Miri and A.K. Khandani, "On structure and decoding of product codes," *IEEE International Symposium in Information Theory*, pp. 86, Sorrento, June 2000.

[16] R.M. Pyndiah, "Near-optimum decoding of product codes: block turbo codes," *IEEE Transactions on Communications*, vol. 46, no. 8, Aug. 1998.

[17] D. Rankin and T.A. Gulliver, "Asymptotic performance of product codes," *IEEE International Conference on Communications*, pp. 431-435, Vancouver, June 1999.

[18] M. Schwartz, P.H. Siegel, and A. Vardy, "On the asymptotic performance of iterative decoders for product codes," *IEEE International Symposium on Information Theory*, pp. 1758-1762, Adelaide, Sept. 2005.

[19] A. Sella and Y. Be'ery, "Convergence analysis of turbo decoding of product codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 723-735, Feb. 2001.

[20] R.M. Tanner,"A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. IT-27, no. 5, pp. 533-547, Sept 1981.

[21] L.M.G.M. Tolhuizen, "More results on the weight enumerator of product codes," *IEEE Transactions on Information Theory*, vol. 48, no. 9, pp. 2537-2577, Sept. 2002.

[22] D.P. Varodayan, "Investigation of the Elias product code construction for the binary erasure channel", B.A.S. Thesis, University of Toronto, Dec. 2002.

[23] L. Xu, V. Bohossian, J. Bruck, and D.G. Wagner, "Low-density MDS codes and factors of complete graphs," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1817-1826, Sept. 1999.