Pseudo-Binomial Degree Distributions from Derivative Matching

Enrico Paolini and Marco Chiani
DEIS / WiLAB, University of Bologna
via Venezia 52, 47023 Cesena (FC), Italy
{e.paolini,marco.chiani}@unibo.it

Marc Fossorier
ETIS ENSEA / UCP / CNRS UMR-8051
6, avenue du Ponceau, 95014, Cergy Pontoise, France
mfossorier@ieee.org

***Abstract*— In this paper, a method to design check-concentrated LDPC degree distributions for the erasure channel is proposed. This method is obtained taking a derivative matching approach. It consists of matching the first and high-order derivatives of the variable node decoder EXIT function and inverse check node decoder EXIT function in order to reduce the gap between the two curves in the EXIT chart. A sufficient condition for a check-concentrated distribution to achieve derivative matching up to some order is first developed, and then a design algorithm is proposed exploiting this sufficient condition. A comparison with other deterministic design techniques is provided, revealing the potentialities of the proposed algorithm.**

I. INTRODUCTION

Currently, the most popular and effective tool for numerical optimization of low-density parity-check (LDPC) code degree distributions is represented by differential evolution (DE) [1], first applied to LDPC codes in [2]. The basic idea is to consider a population of N_p degree distributions, all satisfying common constraints such as code rate and active variable node (VN) and check node (CN) degrees. At each step of the algorithm, a new population is generated from the old one through a recombination operation, in such a way that the maximum among the decoding thresholds is improved.

Among the advantages of DE we can include its fastness (provided that the number of active degrees is not too large), the possibility of using it with different analysis tools, like density evolution [3] or Extrinsic Information Transfer (EXIT) chart [4], its general purpose nature which allows to apply it both to different communication channels and to code structures more general than LDPC codes [5], [6], and the possibility to perform constrained optimizations. Examples of constraints are represented by maximum number of active degrees, bounds on key parameters (such as $\lambda'(0)\rho'(1)$ for LDPC codes), etc. Some drawbacks of DE are a general lack of control over the degree distribution optimization process, its pseudo-randomness which may lead to different final distributions in correspondence with the same initial population, a certain dependence of the returned distribution on the starting population and, more importantly, an optimization time which may become impractical if the number of active degrees becomes too large. It is worthwhile noting that the algorithm pseudo-randomness and its dependence on the starting population are usually not an issue for LDPC degree distributions over the binary erasure channel (BEC).

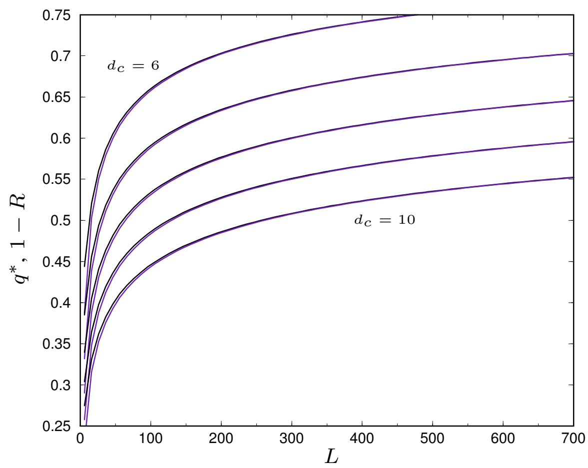

Fig. 1. Binomial degree distribution chart ($d_c = 6, \ldots, 10$). For each value of d_c the upper curve is $1 - R$ and the lower curve is q^*.

For LDPC codes over the BEC solutions different from DE are available for obtaining degree distributions with a good threshold, namely, analytical solutions. The state of the art in this field is represented by [7]–[10]. In [7] and [8] the *binomial* sequence and the *Tornado* sequence were introduced, respectively, both able to achieve the BEC capacity. Slightly modified versions of these two sequences were successively regarded in [9] as special instances of a much more general technique for obtaining capacity achieving sequences for the BEC. A deterministic algorithm for degree distributions optimization is provided in [10] (see also Section IV-C).

The binomial degree distribution introduced in [7] is check-regular and characterized by an edge-oriented VN distribution

$$\lambda(x) = \sum_{i=2}^{L} \frac{\alpha \binom{\alpha}{i-1}(-1)^i}{\alpha - L\binom{\alpha}{L}(-1)^{L+1}} x^{i-1}\,, \quad (1)$$

where L denotes the maximum VN degree, d_c the CN degree, $\alpha \triangleq (d_c - 1)^{-1}$ and $\binom{\alpha}{N} = \alpha(\alpha-1)\ldots(\alpha-N+1)/(N!)$. A chart illustrating the behaviors of $1-R$ (R being the code rate) and the threshold q^* as functions of L and d_c is depicted in Fig. 1, from which it is evident how the q^* curve tightly matches the $1-R$ curve for all the considered values of d_c. A few additional observations are provided next. For each rate R, the larger d_c the closer q^* to $1-R$ (capacity achieving

978-1-4244-2863-2/08/$25.00 © 2008 IEEE

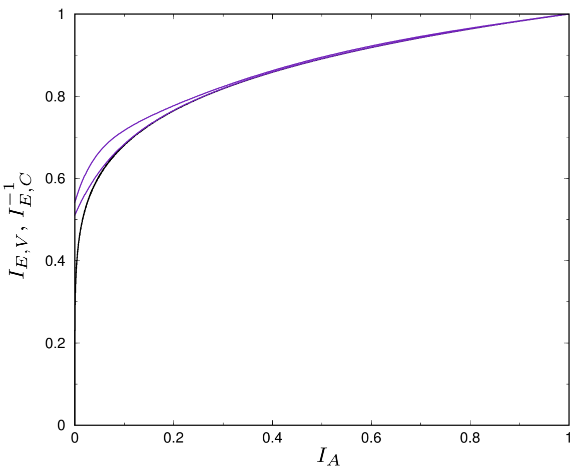

Fig. 2. EXIT chart for two pseudo-binomial distributions with different derivative matching order. The inverse CND EXIT function is the same for the two codes. Upper VND EXIT function: only the first derivative is matched. Lower VND EXIT function: the derivatives are matched up to the order 20.

sequence). For each d_c the gap between q^* and $1-R$ is smaller in the low-rate region ($1 - R > 1/2$), corresponding to larger values of L. For each d_c a small rate reduction in the low rate region corresponds to a very large increase in terms of L.

Since L is an integer, the binomial distribution is capable to match a given code rate approximately. This limitation can be overcome by adopting the construction proposed in [9, Algorithm 1] where a slightly modified version has been obtained by setting $\rho(x) = x^{d_c-1}$ and $\lambda(x)$ equal to a truncated and normalized version of the Taylor series expansion of $1-\rho^{-1}(1-x)$: it can achieve exactly any code rate. In the sequel we need to keep the binomial distribution of [7] and its modified version of [9] distinguished.

In this paper, a class of check-concentrated LDPC degree distributions for the BEC is introduced together with an algorithm for their construction. As these distributions are related to the binomial one, they are here referred to as *pseudo-binomial* distributions. Their construction algorithm is based on the concept of *derivative matching*. According to the area theorem proved in [11], the BEC capacity can be asymptotically approached by matching the variable node decoder (VND) EXIT function $I_{E,V}(I_A, q)$ to the inverse check node decoder (CND) EXIT function $I_{E,C}^{-1}(I_A)$ (q is the BEC erasure probability). Given that both $I_{E,V}(I_A, q)$ and $I_{E,C}^{-1}(I_A)$ are equal to 1 at $I_A = 1$, which holds when the minimum VN and CN degree is at least two, the derivative matching approach consists of trying to match the two EXIT curves by exactly matching their first and high-order derivatives respect to I_A, at $I_A = 1$ and $q = q^*$.

Example 1: Let us consider Fig. 2, where the EXIT charts of two pseudo-binomial distributions are depicted. For each distribution the VND EXIT function is plotted at the corresponding threshold ($q = q^*$). They are both characterized by $R = 1/2$, $d_c = 7$ and $L = 30$, and have been obtained through Algorithm 2 described in Section III. For the distribution with a larger gap between the EXIT curves only the first derivative at $I_A = 1$ is matched: the active degrees are 2, 4, 30, and the threshold is $q^* = 0.458324$. For the other distribution the derivatives are matched up to the order 20, the active degrees are $2, \ldots, 21$, 23, 30, and the threshold is $q^* = 0.490935$.

The derivative matching approach is explained in Section II. It is also shown that, among the check-concentrated distributions, the binomial distribution is optimum in terms of derivative matching. The proposed design method is described in Section III, while numerical results comparing the proposed approach to other deterministic design techniques are provided in Section IV. Concluding remarks are given in Section V.

II. Derivative Matching

Concerning the derivative matching approach, the first problem is the development of a condition under which the first derivative respect to I_A, at $I_A = 1$ and $q = q^*$, is matched. To this end the following result is useful.

Proposition 1: For any degree distribution with $\lambda'(0) > 0$ we have

$$\frac{\partial I_{E,V}(I_A, q^*)}{\partial I_A}\Big|_{I_A=1} = \frac{\mathrm{d}I_{E,C}^{-1}(I_A)}{\mathrm{d}I_A}\Big|_{I_A=1} \tag{2}$$

if and only if $q^* = [\lambda'(0)\rho'(1)]^{-1}$.

Proposition 1 is a straightforward consequence of the fact that, for an LDPC code, $I_{E,V}(I_A, q) = 1 - q\,\lambda(1 - I_A)$ and $I_{E,C}(I_A) = \rho(I_A)$.

For any check-concentrated degree distribution with maximum VN degree L we consider a real polynomial $p(x) = \sum_{n=0}^{L-2} p_n x^n$ whose coefficients are defined as

$$p_n = [(n+1)d_c - (n+2)]\,\lambda_{n+2} - (n+2)(d_c-1)\lambda_{n+3} \tag{3}$$

for $n = 0, \ldots, L-3$ and

$$p_{L-2} = [(L-1)d_c - L]\,\lambda_L\,. \tag{4}$$

This polynomial was introduced in [12]. We show next that it plays a key role within the derivative matching approach. We have the following result from [12].

Proposition 2: For any check-concentrated degree distribution with $\lambda'(0) > 0$, if $p(x) \geq 0$ for all $x \in (0, 1]$ then we have $q^* = [\lambda'(0)\rho'(1)]^{-1} = [\lambda_2\,(d_c - 1)]^{-1}$.

This condition is sufficient but not necessary. Combining Proposition 1 and Proposition 2 we obtain a sufficient condition for (2).

Proposition 3: For any check-concentrated degree distribution with $\lambda'(0) > 0$, if $p(x) \geq 0$ for all $x \in (0, 1]$ then (2) is satisfied.

Proposition 3 represents a simple sufficient condition to guarantee the matching of the first derivative respect to I_A, at $I_A = 1$ and $q = q^*$ [1]. Concerning the higher-order derivatives, we have the following property.

[1]We observe that the first derivative matching condition is equivalent to the *flatness condition* of [13].

Proposition 4: For any check-concentrated degree distribution with $\lambda'(0) > 0$ and such that $p(x) \geq 0$ for all $x \in (0,1]$, $p_i = 0$ for all $i = 0, \ldots, M-2$ if and only if

$$\frac{\partial^{(n)} I_{E,V}(I_A,\, q^*)}{\partial I_A^{(n)}}\Big|_{I_A=1} = \frac{\mathrm{d}^{(n)} I_{E,C}^{-1}(I_A)}{\mathrm{d} I_A^{(n)}}\Big|_{I_A=1} \quad (5)$$

for all $n = 2, \ldots, M$.

Proof: We have

$$\frac{\partial^{(n)} I_{E,V}(I_A,\, q)}{\partial I_A^{(n)}}\Big|_{I_A=1} = (-1)^{n+1}\,(n!)\,q\,\lambda_{n+1}$$

and

$$\frac{\mathrm{d}^{(n)} I_{E,C}^{-1}(I_A)}{\mathrm{d} I_A^{(n)}}\Big|_{I_A=1} = \prod_{j=0}^{n-1}\left(\frac{1}{d_c-1} - j\right).$$

Assume that $p(x) \geq 0$ for all $x \in (0,1]$ (which ensures matching of the first derivative by Proposition 3) and that (5) holds for $n = 2, \ldots, M$. For each n we obtain

$$(n!)\,q^*\,\lambda_{n+1} = \frac{1}{d_c-1}\prod_{j=1}^{n-1}\left(j - \frac{1}{d_c-1}\right),$$

that is

$$\frac{\lambda_{n+1}}{\lambda_2} = \frac{1}{n!}\prod_{j=1}^{n-1}\left(j - \frac{1}{d_c-1}\right), \quad (6)$$

where the latter expression follows from Proposition 2. For $n = 2$, (6) implies $p_0 = 0$. For $n \geq 3$ we can write (6) for the order $n-1$ and divide term by term. This leads to

$$\frac{\lambda_{n+1}}{\lambda_n}\,n = n - 1 - \frac{1}{d_c-1},$$

which implies $p_{n-2} = 0$.

Conversely, we assume that $p(x) \geq 0$ for all $x \in (0,1]$ and that $p_i = 0$ for all $i = 0, \ldots, M-2$. From $p_0 = 0$ we obtain (6) with $n = 2$, which is equivalent to (5) with $n = 2$ through Proposition 2. For $i \geq 3$ we can combine $p_i = 0$ with $p_{i-1} = 0$ to obtain (6) with $n = i+2$. Through Proposition 2 this leads to (5) with $n = i+2$. □

In conclusion, the polynomial $p(x)$ provides a sufficient condition for check-concentrated distributions obtained from derivative matching. If $p(x) \geq 0$ for all $x \in (0,1]$ and t is the smallest degree among the non-zero terms of $p(x)$, then all the derivatives are matched up to the order $t+1$.

This discussion offers simple guidelines for degree distribution design over the BEC. Specifically, we can look for check-concentrated distributions with $p(x)$ non-negative in $(0,1]$ and having the power of the first non-null term as large as possible. The following algorithm forces the matching of the derivatives up to the order $L-1$.

Algorithm 1:

(a) Select d_c and L.
(b) For all $n = 2, \ldots, L-1$ set $\lambda_{n+1} = \lambda_{n+1}(\lambda_2)$ according to (6).
(c) Find λ_2 such that $\lambda_2 + \sum_{n=3}^{L} \lambda_n(\lambda_2) = 1$.

This algorithm generates a check-concentrated degree distribution with CN degree d_c, maximum VN degree L and with $0 < \lambda_L < \cdots < \lambda_2$. All the derivatives are matched up to the order $L-1$: this can be easily recognized by noting that $p(x) = p_{L-2}\,x^{L-2} > 0$ for all $x \in (0,1]$ by construction.

Proposition 5: The ensemble of check concentrated distributions generated by Algorithm 1 coincides with the ensemble of the binomial distributions of [7].

Proof: For given d_c and L, each polynomial $p(\cdot)$ is associated with one and only one VN distribution $\lambda(x)$. In fact, as $p(x)$ has $L-1$ coefficients, for any given $p(x)$ we obtain $L-1$ equations in the $L-1$ unknowns $\lambda_2, \ldots, \lambda_L$. It is readily shown that for any pair (d_c, L) the corresponding binomial distribution, with $\lambda(x)$ specified in (1), is characterized by $p(x) = p_{L-2}\,x^{L-2}$. Then, for any pair (d_c, L), the binomial distribution and the distribution generated by Algorithm 1 share the same $p(x)$. □

From Proposition 5 we observe that, among the class of check-concentrated distributions, the binomial distributions of [7] are optimum from the viewpoint of EXIT curves derivative matching. However, for given d_c and L, achieving this optimum is not compatible with a further code rate constraint: R is a function of d_c and L, denoted by $R_b(d_c, L)$ in the following. Since one usually wishes to obtain a good distribution for a given code rate R, a possible approach may consist of using the chart in Fig. 1 to find the most suitable L for given d_c and R: however, as the values of L are integer, R can be usually only approximated. In the next section, pseudo-binomial distributions are introduced as a possible solution for achieving a code rate exactly within the framework of the derivative matching approach.

III. Pseudo-Binomial Degree Distributions

Let us recall that, if $p(x) \geq 0$ for all $x \in (0,1]$ (first derivative matched), then a high order derivative matching can be achieved by (6). We need a criterion for the non-negativity of $p(x)$ in $(0,1]$. This problem was considered in [12], where the following result was obtained.

Proposition 6: Given a check-concentrated distribution with $\lambda_2 > 0$, a necessary condition for $p(x)$ to be non-negative for all $x \in (0,1]$ is that the number of sign changes in the sequence $p_0, p_1, \ldots, p_{L-2}$ is even.

The proof is based on the Fourier-Budan theorem, a generalization of the Descartes' rule of signs. By Proposition 6, the check-concentrated distributions with $p(x)$ non-negative in $(0,1]$ must be searched in the ensemble of distributions whose associated $p(x)$ has an even number of sign changes in the sequence $p_0, p_1, \ldots, p_{L-2}$. The condition established by Proposition 6, though very simple, is however not sufficient: there exist check-concentrated distributions fulfilling the above condition but for which $p(x)$ has real roots in $(0,1]$.

Definition 1: We call a *pseudo-binomial* degree distribution any check-concentrated distribution with active degrees $2, \ldots, M+1, K, L$, with $M+3 \leq K \leq L-2$, such that the EXIT function derivatives (respect to I_A, at $I_A = 1$ and $q = q^*$) are matched up to the order M.

The expression pseudo-binomial is used as, from $n = 3$ up to $n = M + 1$, we have the same dependence $\lambda_n(\lambda_2)$ as for the binomial distribution. For these distributions the only non-zero coefficients of $p(x)$ are

$$\begin{aligned}
p_{M-1} &= [M d_c - (M+1)]\lambda_{M+1} > 0 \\
p_{K-3} &= -[(K-1)d_c - (K-1)]\lambda_K < 0 \\
p_{K-2} &= [(K-1)d_c - K]\lambda_K > 0 \\
p_{L-3} &= -[(L-1)d_c - (L-1)]\lambda_L < 0 \\
p_{L-2} &= [(L-1)d_c - L]\lambda_L > 0 \,,
\end{aligned}$$

implying that, independently of d_c and $\lambda(x)$, there are always four sign changes in the sequence $p_0, p_1, \ldots, p_{L-2}$.

The reason for considering $2, \ldots, M+1$, K and L, with $M + 3 \le K \le L - 2$, as the active VN degrees can be justified as follows. The CN degree d_c, the maximum and intermediate VN degrees L and K, the code rate R and the derivative matching order M are taken here as the input for the distribution optimization problem. Provided that the first derivative is matched, in order to match the high-order derivatives up to the order M it is necessary and sufficient to impose (6) for $n = 2, \ldots, M$ so that $\lambda_n = \lambda_n(\lambda_2)$ for $n = 3, \ldots, M+1$. Through the constraints

$$\sum_{n=2}^{L} \lambda_n = 1 \tag{7}$$

$$\sum_{n=2}^{L} \lambda_n / n = [(1-R)\, d_c]^{-1} \,, \tag{8}$$

the latter representing the code rate constraint, we obtain $\lambda_K = \lambda_K(\lambda_2)$ and $\lambda_L = \lambda_L(\lambda_2)$. The last step consists in searching the value of λ_2 fulfilling the condition $p(x) \ge 0$ for all $x \in (0, 1]$, and providing the best possible threshold q^*. Using the above mentioned active VN degrees simplifies this latter task, as it guarantees that the number of sign changes in the sequence $p_0, p_1, \ldots, p_{L-2}$ is even. The proposed algorithm for pseudo-binomial distributions construction is formalized next. The set of active VN degrees is denoted by $\mathcal{D} \triangleq \{2, \ldots, M+1, K, L\}$, while the set of non-active degrees by $\overline{\mathcal{D}}$.

Algorithm 2:

(a) Select d_c, L, M, K and R.

(b) Set

$$\lambda_2(\varepsilon) = [(1-\varepsilon)(1-R)(d_c - 1)]^{-1}$$

and, for $n = 3$ to $n = M + 1$,

$$\lambda_n(\varepsilon) = \frac{\lambda_2(\varepsilon)}{(n-1)!} \prod_{j=1}^{n-2} \left(j - \frac{1}{d_c - 1} \right) .$$

(c) Set

$$\begin{aligned}
\lambda_K(\varepsilon) &= \frac{K\,[-a(\varepsilon) + L\, b(\varepsilon)]}{K - L} \\
\lambda_L(\varepsilon) &= \frac{L\,[-a(\varepsilon) + K\, b(\varepsilon)]}{K - L}
\end{aligned}$$

where

$$\begin{aligned}
a(\varepsilon) &\triangleq 1 - \sum_{n=2}^{M+1} \lambda_n(\varepsilon) \\
b(\varepsilon) &\triangleq \frac{1}{(1-R)\, d_c} - \sum_{n=2}^{M+1} \frac{\lambda_n(\varepsilon)}{n} \,.
\end{aligned}$$

(d) Find the solutions $\mathcal{E}$ of the system of inequalities

$$\begin{cases} 0 < \varepsilon < 1 \\ 0 < \lambda_2(\varepsilon) < 1 \\ 0 < \lambda_K(\varepsilon) < 1 \\ 0 < \lambda_L(\varepsilon) < 1 \,. \end{cases}$$

If $\mathcal{E} = \emptyset$, exit and declare a failure.

(e) Find the real solutions $(\overline{x}, \overline{\varepsilon})$ of

$$\begin{cases} p\,(x; \varepsilon) = 0 \\ p'(x; \varepsilon) = 0 \end{cases}$$

such that $\overline{x} \in (0, 1)$ and $\overline{\varepsilon} \in \mathcal{E}$. If no such solution exists, exit and declare a failure.

(f) Set $\varepsilon_{opt} = \max\{\overline{\varepsilon}\}$. If there exists some $0 < \alpha < 1$ such that $p\,(\alpha; \varepsilon_{opt}) < 0$ and $p'(\alpha; \varepsilon_{opt}) = 0$, exit and declare a failure. Else, set $\lambda_n = \lambda_n(\varepsilon_{opt})$ for $n \in \mathcal{D}$, $\lambda_n = 0$ for $n \in \overline{\mathcal{D}}$, and declare a success.

The returned distribution is characterized by EXIT function derivatives matched up to the order M, and by a threshold

$$q^*(\varepsilon_{opt}) = (1 - \varepsilon_{opt})(1 - R).$$

Let us explain the algorithm next. The threshold q^* is expressed as $q^*(\varepsilon) = (1-\varepsilon)(1-R)$ for $0 < \varepsilon < 1$. As the objective distribution has a non-negative $p(x)$ in $(0, 1]$, Proposition 2 implies $q^* = [\lambda_2\,(d_c - 1)]^{-1}$. This leads to the first setting at step (b), while the second setting coincides with (6) up to the order M. Note that there exists a one-to-one correspondence between λ_2 and ε. The settings at step (c) allow to fulfill the constraints (7) and (8). All the terms of the distribution are now expressed as functions of ε. Step (d) provides a permitted region $\mathcal{E}$ for ε (here it is worthwhile noting that $0 < \lambda_2 < 1$ implies $0 < \lambda_n(\lambda_2) < 1$ for all $n = 3, \ldots, M+1$). The goal is to find the smallest ε such that $p\,(x; \varepsilon) \ge 0$ for all $x \in (0, 1]$ given the boundaries (b), (c) and (d), where the notation $p\,(x; \varepsilon)$ makes the dependence of the $p(x)$ coefficients on ε explicit. This task is accomplished by searching the largest $\varepsilon \in \mathcal{E}$ (denoted by ε_{opt}) such that the graph of $p(x)$ is tangent to the abscissa axis for some $\overline{x} \in (0, 1)$.

For a selected set of input parameters, a degree distribution with non-negative $p(x)$ and fulfilling (6) for $n = 2, \ldots, M$ may not exist. In this situation one of the steps (d), (e) or (f) is unsuccessful. Note that, even if the steps (d) and (e) are successful, $p(x)$ could have real roots in $(0,1]$ for $\varepsilon = \varepsilon_{opt}$. Since $p(1) > 0$ and $p(0) \geq 0$[2] the existence of such roots can be checked only focusing on the local minima.

It is worthwhile remarking that the Area Theorem from [11] imposes the matching of an increasing number of derivatives to achieve the BEC capacity. For this reason, pseudo-binomial distributions converge to the binomial ones as the gap to capacity tends to zero. Pseudo-binomial distributions can then be interpreted as a correction factor to the distributions from [7] leading to a better efficiency for finite gap to capacity[3].

Numerical results are presented in the next section. Even if the intermediate degree K is potentially a degree of freedom for the design, we always assume $K = M + 3$ next for simplicity.

IV. Numerical Results

A. Derivative Matching Order and Optimization Time

It has been pointed out in Section II that achieving the optimum derivative matching order constrains the code rate, which becomes a function $R_b(d_c, L)$ of d_c and L if the derivatives are matched up to the order $L-1$. With pseudo-binomial distributions, a given set of active degrees d_c and $\mathcal{D}$ is associated with a set of permitted code rates. In general, the larger the derivative matching order the smaller the permitted rate region. This permitted rate region includes $R_b(d_c, L)$.

Example 2: We select $d_c = 8$ and $L = 60$. The corresponding binomial distribution has a code rate $R_b(8, 60) = 0.500352 \simeq 1/2$ (see also Fig. 1). For the same values of d_c and L, and for $R = 1/2$, Algorithm 2 is successful up to a derivative matching order $M = 55$. However, with $M = 55$ Algorithm 2 is not successful for both $R = 0.51$ and $R = 0.49$, which values of R can be achieved for $M \leq 37$. Furthermore, for achieving $R = 0.52$ and $R = 0.48$ it is necessary to select $M \leq 33$.

In conclusion, given d_c and L, the maximum derivative matching order M depends on the code rate. Values of R close to $R_b(d_c, L)$ are more favorable for derivative matching.

The optimization time depends on the input parameters. Over a standard processor, we found optimization times ranging from a few seconds to a few minutes. For example, selecting $L = 60$, $d_c = 8$, $R = 1/2$ and $M = 30$ the optimization time was about 3 seconds. With $L = 200$, $d_c = 8$, $R = 0.4$ and $M = 148$ the optimization required about 47 seconds, while with $L = 600$, $d_c = 8$, $R = 0.35$ and $M = 221$ the optimization required 3 minutes and 20 seconds.

B. Low-Rate Distributions

Observing Fig. 1 we notice that an optimum derivative matching imposes to select very large values of L for achieving code rates $R < 1/2$. The same feature is shared by the right-regular distribution proposed in [9]. In this subsection we show that pseudo-binomial distributions can be used to mitigate this phenomenon, while maintaining values of q^* close to $1 - R$.

Let us consider Fig. 3, where the binomial curve for $d_c = 8$ is depicted in the low-rate region. In the same graph additional points are shown for $R = 0.45$, $R = 0.4$ and $R = 0.35$ which correspond to pseudo-binomial distributions with $d_c = 8$. Each pseudo-binomial distribution achieves the same rate as its binomial counterpart with a much smaller value of L, while preserving a threshold very close to $1-R$. For example, for point 1 we have $(L_1, M_1) = (400, 221)$, $1-R = 0.65$ and threshold $q_1^* = 0.649657$, whereas the binomial counterpart is characterized by $L = 764$, $1 - R = 0.650005$ and $q^* = 0.649707$. It is worthwhile remarking that, in this case, the binomial distribution has 763 active VN degrees, while the pseudo-binomial one has 223 active degrees, which implies a simpler implementation.

In Table I we compare $R = 1/3$ pseudo-binomial distributions with $R = 1/3$ right-regular distributions from [9] for $d_c = 6$, 7 and 8. Each value of M shown in the table represents the largest derivative matching order compatible with the given d_c, L and R. This example illustrates the capability of the pseudo-binomial approach to achieve a low code rate with a reduced maximum VN degree. In some cases, the threshold obtained with Algorithm 2 can be better than the threshold of

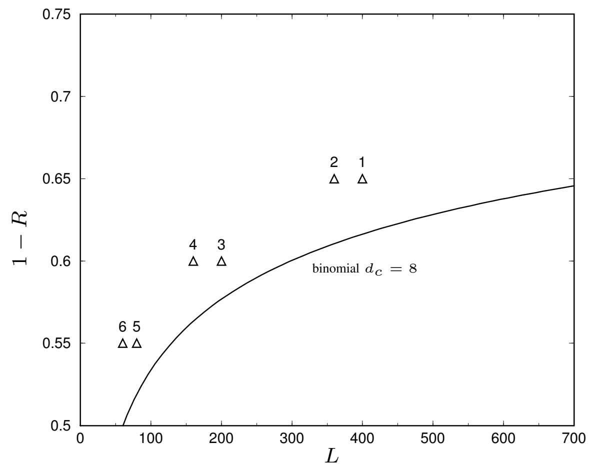

Fig. 3. Binomial and pseudo-binomial distributions with $d_c = 8$ in the low-rate region. $(L_1, M_1) = (400, 221)$, $(L_2, M_2) = (360, 155)$, $(L_3, M_3) = (200, 148)$, $(L_4, M_4) = (160, 91)$, $(L_5, M_5) = (80, 53)$, $(L_6, M_6) = (60, 24)$. Thresholds: $q_1^* = 0.649657$, $q_2^* = 0.649460$, $q_3^* = 0.599225$, $q_4^* = 0.599116$, $q_5^* = 0.548134$, $q_6^* = 0.546397$.

TABLE I

Rate-$1/3$ degree distributions.

	right-regular [9]		*pseudo-binomial*		
	L	q^*	L	M	q^*
$d_c = 6$	111	0.664649	75	55	0.664733
$d_c = 7$	349	0.666029	230	168	0.666054
$d_c = 8$	1078	0.666460	600	360	0.666452

[2] If $M = 1$ then $\lambda_3 = 0$ and $p_0 > 0$. On the other hand, if $M \geq 2$ then $p_0 = 0$ by construction.

[3] As commented by one of the Reviewers, when the gap to capacity tends to zero the graphical complexity of any LDPC capacity-achieving sequence must tend to infinity [14]. However, LDPC code ensembles have been designed achieving the channel capacity with a bounded complexity [15], [16].

the right-regular distribution from [9] despite the smaller value of L. Degree distributions with even smaller L can be designed with Algorithm 2, still exhibiting a competitive threshold. For example, selecting $L = 60$ and $M = 34$ with $d_c = 6$ we obtain a $R = 1/3$ distribution with $q^* = 0.664479$.

C. Comparison with the Distributions from [10]

A technique for designing LDPC erasure distribution matching a given code rate R exactly was introduced in [10]. Next, we compare this technique (applied to check-regular distributions) and Algorithm 2. The algorithm proposed in [10] accepts as input the CN degree d_c, an intermediate VN degree P, the maximum VN degree L and the code rate R. A rate-R distribution is returned with active VN degrees $2, \dots, P$ and L. First, (6) is imposed for $n = 2, \dots, P-1$, thus obtaining $\lambda_n = \lambda_n(\lambda_2)$ for $n = 3, \dots, P$. Then, λ_L is expressed as a function of λ_2 through the constraint (7). Finally, λ_2 is computed in order to fulfill (8). For given d_c and R, the maximum VN degree L can in principle range between a maximum and a minimum value: it is shown in [10] that the minimum value of L is always the best choice.

This algorithm is computationally less complex than Algorithm 2, and exploits the same dependence between λ_n and λ_2, for n ranging from 3 to P. A difference with respect to Algorithm 2 is that this technique does necessarily return a degree distribution with derivatives matched up to the order $P-1$, as there is no control on the first derivative (note that selecting $2, \dots, P, L$ as the active degrees and imposing (6) for $n = 2, \dots, P$ there are always two sign changes in $p_0, \dots, p_{L-2}$ so that Proposition 6 is satisfied).

Example 3: Selecting $d_c = 6$, $L = 13$, $P = 6$ and $R = 1/2$ we obtain with the algorithm of [10] a distribution with threshold $q^* = 0.489084$. It is readily shown that the first derivative is not matched: in fact we have $[\lambda_2(d_c - 1)]^{-1} = 0.491669$. In this case $p(x)$ has two real roots in $(0, 1]$.

We compared the thresholds of the distributions returned by Algorithm 2 and by the algorithm from [10] for the same d_c and L. To stay fair, we always considered the same number of active degrees. We found in some cases a better threshold with Algorithm 2, while in other cases a better threshold with the approach from [10]. For example, selecting $d_c = 6$, $R = 1/2$, $L = 8$ (this is the minimum L allowed by [10] for the given d_c and R) and taking 4 active degrees (meaning $P = 4$ and $M = 2$, respectively) we obtain $q^* = 0.468800$ with the algorithm from [10] and $q^* = 0.475099$ with Algorithm 2. Selecting $d_c = 6$, $R = 0.4$, $L = 29$ (minimum L) and taking 21 active degrees ($P = 21$ and $M = 19$, respectively) we obtain $q^* = 0.594581$ with the algorithm from [10] and $q^* = 0.594605$ with Algorithm 2. On the other hand, for $L = 15$, $d_c = 7$, $R = 1/2$ and 8 active degrees, we have $q^* = 0.489166$ with the algorithm from [10] and $q^* = 0.488884$ with Algorithm 2.

V. Conclusion

In this paper, we presented an algorithm for generating good check-regular LDPC degree distributions for the erasure channel. The method was developed assuming a derivative matching perspective. Given the CN degree, the maximum VN degree and the code rate, the algorithm returns a degree distribution with optimized threshold and such that the derivatives of the EXIT functions are matched up to a desired order. The proposed algorithm exploits a simple sufficient condition for a check-concentrated distribution to fulfill the derivative matching up to some order. The algorithm was compared with other available optimization techniques. We showed that, under the same set of constraints, the algorithm can return distributions with a better threshold or with a competitive threshold and a smaller number of active degrees. The latter feature looks interesting especially in the low rate region.

Acknowledgment

The work was supported in part by the EC under Seventh FP grant agreement ICT OPTIMIX n.INFSO-ICT-214625.

References

[1] K. Price and R. Storn, "Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces," *J. Global Optimization*, vol. 11, pp. 341–359, 1997.

[2] M. A. Shokrollahi and R. Storn, "Design of efficient erasure codes with differential evolution," in *Proc. of 2000 IEEE Int. Symp. on Information Theory*, Sorrento, Italy, June 2000.

[3] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[4] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[5] E. Paolini, M. Fossorier, and M. Chiani, "Generalized and doubly-generalized LDPC codes with random component codes for the binary erasure channel," *IEEE Trans. Inform. Theory*, 2007, submitted.

[6] Y. Wang and M. Fossorier, "Doubly generalized LDPC codes over the AWGN channel," *IEEE Trans. Commun.*, 2007, to appear.

[7] M. A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity," in *Proc. of Int. Symp. Applied Algebra, Algebraic Algoritmhs, and Error Correcting Codes (Lecture Notes in Computer Science),* M. Fossorier, H. Imai, S. Lin and A. Poli, Eds. Berlin, Germany: Springer-Verlag, 1999, pp. 65–76.

[8] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 569–584, Feb. 2001.

[9] P. Oswald and M. A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 12, pp. 364–373, Dec. 2002.

[10] H. Saeedi and A. H. Banihashemi, "Deterministic design of low-density parity-check codes for binary erasure channels," in *Proc. of 2007 IEEE Global Telecommunications Conf.*, Washington, USA, Nov. 2007, pp. 1566–1570.

[11] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: Model and erasure channel properties," *IEEE Trans. Inform. Theory*, vol. 50, no. 11, pp. 2657–2673, Nov. 2004.

[12] E. Paolini and M. Chiani, "A class of LDPC erasure distributions with closed-form threshold expression," in *Proc. of 2007 IEEE Int. Conf. on Communications*, Glasgow, Scotland, June 2007, pp. 659–664.

[13] M. Shokrollahi, *Capacity-Achieving Sequences*. Minneapolis, USA: Inst. Mathematics and its Applications (IMA), vol. 123, IMA Volumes in Mathematics and its Applications, pp. 153–166, 2000.

[14] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 7, pp. 1611–1635, July 2003.

[15] H. Pfister, I. Sason, and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *IEEE Trans. Inform. Theory*, vol. 51, no. 7, pp. 2352–2379, July 2003.

[16] H. Pfister and I. Sason, "Accumulate-repeat-accumulate codes: Capacity-achieving ensembles of systematic codes for the erasure channel with bounded complexity," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2088–2115, June 2007.