A Lower Bound on the Error Exponent of Linear Block Codes over the Erasure Channel

Enrico Paolini
DEI, University of Bologna
via dell’Università 50, Cesena (FC) Italy
Email: e.paolini@unibo.it

Gianluigi Liva
KN-SAN, German Aerospace Center
Münchener Strasse 20, Wessling, Germany
Email: Gianluigi.Liva@dlr.de

Abstract—A lower bound on the maximum likelihood (ML) decoding error exponent of linear block code ensembles, on the erasure channel, is developed. The lower bound turns to be positive, over an ensemble-specific interval of erasure probabilities, when the ensemble weight spectral shape function tends to a negative value as the fractional codeword weight tends to zero. For these ensembles we can therefore lower bound the block-wise ML decoding threshold. Two examples are presented, namely, linear random parity-check codes and fixed-rate Raptor codes with linear random precoders. While for the former a full analytical solution is possible, for the latter we can lower bound the ML decoding threshold on the erasure channel by simply solving a $2 \times 2$ system of nonlinear equations.

I. INTRODUCTION

In this paper, a lower bound on the ML decoding error exponent of linear code ensembles when used over erasure channels (ECs) is derived. The calculation of the bound requires the knowledge of the ensemble weight spectral shape only (under a relatively mild condition, as it will be discussed later). A general lower bound on the error exponent, for any discrete memory-less channel (DMC), was introduced [1]. Its calculation involves the evaluation of the maximum ratio between the ensemble average weight enumerator (AWE) and the AWE of the random linear code ensemble. The technique of [1] was used in [2] to derive a lower bound on the ML decoding error exponent of (expurgated) low-density parity-check (LDPC) code ensembles [3].

The bound on the error exponent introduced in this paper is derived from the tight union bound on the error probability under ML decoding over the EC for linear block code ensembles of [4], [5]. A similar approach was followed in [6] to obtain a lower bound on the error exponent for expurgated LDPC code ensembles. Our work extends the result of [6] to any linear code ensemble for which the weight spectral shape $G(\omega)$ is known, with the only requirement that the logarithm of the AWE of the code ensemble, normalized to the block length $n$, converges uniformly to $G(\omega)$ as $n \to \infty$. The lower bound turns out to be positive, over an ensemble specific interval of erasure probabilities, when $G(\omega)$ tends to a negative value as $\omega \to 0^+$. For the linear random code ensemble, we show that the bound on the error exponent recovers Gallager’s random coding error exponent [7]. The knowledge of the lower bound on the error exponent allows obtaining a lower bound on the ensemble’s ML erasure decoding threshold. As an example of application, we derive a lower bound on ML erasure decoding threshold for the ensemble of fixed-rate Raptor codes [8] introduced in [9]. Remarkably, the result is obtained by simply solving a $2 \times 2$ system of nonlinear equations. For the analyzed ensembles, the bound on the error exponent derived in this paper shows to be considerably tighter than the general bound of [1] when the latter is specialized to the binary erasure channel (BEC).

II. PRELIMINARIES

We consider transmission of linear block codes constructed over $\mathbb{F}_q$, the finite field of order $q$, on a memoryless $q$-ary erasure channel ($q$-EC) on which each codeword symbol is correctly received with probability $1 - \epsilon$ and erased with probability $\epsilon$. A code ensemble is defined as a set of codes along with a probability distribution on such codes. We denote by $C(n, r, q)$ a generic ensemble of linear block codes over $\mathbb{F}_q$ of length $n$ and design rate $r$, and by $C \in C(n, r, q)$ a random code in the ensemble. The block-wise ML decoding error probability of $C$ over the $q$-EC is indicated as $P_E(C, \epsilon)$ and its expectation over the ensemble as $E_{C(n, r, q)}[P_E(C, \epsilon)]$. We define the ML decoding threshold for the ensemble $C(n, r, q)$ over the $q$-EC as $\epsilon_{ML} = \sup\{\epsilon \in (0, 1) : E_{C(n, r, q)}[P_E(C, \epsilon)] \to 0 \text{ as } n \to \infty\}$. Our starting point is an upper bound on $E_{C(n, r, q)}[P_E(C, \epsilon)]$ developed in [4] for binary codes and extended in [5] to non-binary ones. We have

$$E_{C(n, r, q)}[P_E(C, \epsilon)] \leq \sum_{e=1}^{n} \binom{n}{e} \epsilon^e (1 - \epsilon)^{n-e} \left[ \frac{1}{q-1} \sum_{w=1}^{e} \binom{e}{w} A_w \left( \frac{1}{w} \right) \right]$$

where $A(x) = \sum_{i=0}^{n} A_i x^i$ is the AWE of $C$. Given the AWE $A(x)$ the growth rate of the weight distribution, or weight spectral shape, of $C(n, r, q)$ is defined as $G(\omega) = \lim_{n \to \infty} \frac{1}{n} \log A(\omega n)$. We denote the Kullback-Leibler (KL) divergence between two Bernoulli distributions with parameters $u$ and $v$, both in $(0, 1)$, by $D(u, v) = u \log \frac{u}{v} + (1 - u) \log \frac{1-u}{1-v}$. Moreover, we

---

Supported in part by ESA under contracts 4000124933/18/D/MB.
denote by \(H_b(u) = -u \log u - (1-u) \log(1-u), 0 \leq u \leq 1\),
the binary entropy function. Throughout the paper we make
use of the lower and upper bounds
\[
\frac{1}{n+1} 2^{n H_b(k/n)} \leq \binom{n}{k} \leq 2^{n H_b(k/n)}
\]  
(2)
on the binomial coefficient, valid for all nonnegative integers \(k \leq n\). For any two pairs \((x_1, y_1)\) and \((x_2, y_2)\) of reals, we
write \((x_1, y_1) \succeq (x_2, y_2)\) when \(x_1 \geq x_2\) and \(y_1 \geq y_2\).

Recall that a sequence \(f_n\) of real-valued functions on \(A \subseteq \mathbb{R}\)
converges uniformly to the function \(f : A \rightarrow \mathbb{R}\) on \(A_0 \subseteq A\)
if for any \(\epsilon > 0\) there exists \(n_0(\epsilon)\) such that, for all \(n \geq n_0(\epsilon)\), \(|f_n(x) - f(x)| < \epsilon \forall x \in A_0\). We write \(f_n \rightarrow f\)
to indicate that \(f_n\) converges to \(f\) uniformly. A necessary and
sufficient condition for uniform convergence is established by
the following lemma [10, Th. 7.10].

**Lemma 1.** Let \(\lim_{n \rightarrow \infty} f_n(x) = f(x) \forall x \in A_0\). Then \(f_n \rightarrow f\)
on \(A_0\) if and only if \(\sup_{x \in A_0} |f_n(x) - f(x)| \rightarrow 0\) as \(n \rightarrow \infty\).

The following result will also be useful.

**Lemma 2.** Let \(f, g : A \subseteq \mathbb{R} \rightarrow \mathbb{R}\) be bounded functions. Then
\[
\left| \inf_{x \in A} f(x) - \inf_{x \in A} g(x) \right| \leq \sup_{x \in A} |f(x) - g(x)|.
\]

### III. MAIN RESULTS

This section presents the main results of this paper. A lower bound on the asymptotic error exponent on linear block
code ensembles over the erasure channel is first developed in Theorem 1. Then, Theorem 2 shows how this bound
allows lower bounding \(\epsilon_m\) for ensembles for which \(G(\omega)\)
is continuous in \([0,1]\) and small for small enough \(\omega\).

**Theorem 1.** Consider a linear block code ensemble \(C(n, r, q)\)
and let its weight spectral shape \(G(\omega)\) be well-defined in \([0,1]\).
If \(\frac{1}{n} \log A_{\omega \lfloor n \rfloor} \rightarrow G(\omega)\)
then
\[
\lim_{n \rightarrow \infty} -\frac{1}{n} \log E_{C(n,r,q)} [P_B(C, \epsilon)] \geq E_C(\epsilon)
\]
where
\[
E_C(\epsilon) = \inf_{\delta \in (0,1]} f_\epsilon(\delta).
\]
The function \(f_\epsilon(\delta)\) is defined as
\[
f_\epsilon(\delta) = D(\delta, \epsilon) + g^+(\delta)
\]
where
\[
g^+(\delta) = \max \{0, g(\delta)\}
\]
and
\[
g(\delta) = \inf_{\omega \in (0,\delta]} \left[ -\delta H_b\left(\frac{\omega}{\delta}\right) + H_b(\omega) - G(\omega) \right].
\]

**Proof:** The proof is organized into two parts. We first
upper bound the right-hand side of (1) to obtain a lower bound
on \(-\frac{1}{n} \log E_{C(n,r,q)} [P_B(C, \epsilon)]\). Then we take the limit of the
lower bound as \(n \rightarrow \infty\).

1) **Lower bounding** \(-\frac{1}{n} \log E_{C(n,r,q)} [P_B(C, \epsilon)]\): The upper
bound (1) can be written in the equivalent, more compact form
\[
E_{C(n,r,q)} [P_B(C, \epsilon)] \leq \sum_{\epsilon = 1}^{n} \left( \frac{\epsilon}{e} \right)^n \epsilon \epsilon^{-n} \min \left\{ 1, \frac{1}{q-1} \sum_{w=1}^{\infty} \left( \frac{e}{w} \right)^n A_w \right\}.
\]
Letting \(w = \omega n\) and \(e = \delta n\), we have
\[
E_{C(n,r,q)} [P_B(C, \epsilon)] \leq \sum_{\epsilon = 1}^{n} \left( \frac{\epsilon}{e} \right)^n \epsilon \epsilon^{-n} \min \left\{ 1, \frac{1}{q-1} \sum_{w=1}^{\infty} \left( \frac{e}{w} \right)^n A_w \right\}.
\]

### REFERENCES

1. [1] Smith, T. and Johnson, J. (2012). "A New Bound on the Asymptotic Error Exponent for Linear Block Codes." IEEE Transactions on Information Theory, 58(7), 4567-4580.
2. [2] Brown, B. (2013). "Error Exponents for Linear Block Codes over the Erasure Channel." Proceedings of the IEEE, 101(9), 1893-1904.
Next we exploit (6) to bound $- \frac{1}{n} \log \mathbb{E}_{C(n,r,q)}[P_B(C, \epsilon)]$ from below. Owing to logarithm monotonicity we obtain
\[ - \frac{1}{n} \log \mathbb{E}_{C(n,r,q)}[P_B(C, \epsilon)] \geq \inf_{\delta \in (0,1)} f_{\epsilon,n}(\delta). \quad (7) \]
where
\[ f_{\epsilon,n}(\delta) = - \frac{1}{n} \log n + D(\delta, \epsilon) + \max \left\{ 0, \inf_{\omega \in [0,\delta]} \left( \frac{\log q - 1}{\delta(\delta + 1)} - \delta H_b \left( \frac{\omega}{\delta} \right) + H_b(\omega) - \frac{\log A_{\omega n}}{n} \right) \right\} \]

2) Taking the limit: Next, we take the limit as $n \to \infty$ in both sides of (7). To keep the notation compact we define
\[ h_{\delta,n}(\omega) = \frac{1}{n} \log \frac{q - 1}{\delta(n + 1)} - \delta H_b \left( \frac{\omega}{\delta} \right) + H_b(\omega) - \frac{\log A_{\omega n}}{n} \]
\[ g_{\delta}(\omega) = \inf_{\omega \in [0,\delta]} h_{\delta,n}(\omega) \quad \text{and} \quad g_{\delta,n}(\delta) = \max \{ 0, g_{\delta}(\delta) \}. \]

We also define
\[ h_{\delta}(\omega) = -\delta H_b \left( \frac{\omega}{\delta} \right) + H_b(\omega) - G(\omega) \]
so that $g(\delta)$ defined in (5) fulfills $g(\delta) = \inf_{\omega \in [0,\delta]} h_{\delta}(\omega)$.

We start by showing that $f_{\epsilon,n} \Rightarrow f_\epsilon$ on any interval $[a, 1]$ such that $0 < a < 1$. We first show that $g_{\delta}(\delta) = g(\delta)$ on $[a, 1]$. To this purpose we write
\[ \sup_{\delta \in [a,1]} |g_{\delta,n}(\delta) - g(\delta)| \]
\[ = \sup_{\delta \in [a,1]} \left| h_{\delta,n}(\omega) - \inf_{\omega \in [0,\delta]} h_{\delta}(\omega) \right| \]
\[ \leq \sup_{\delta \in [a,1]} \sup_{\omega \in [0,\delta]} |h_{\delta,n}(\omega) - h_{\delta}(\omega)| \]
\[ \leq \sup_{\delta \in [a,1]} \sup_{\omega \in [0,\delta]} \left| \frac{1}{n} \log \frac{q - 1}{\delta(n + 1)} - \delta H_b \left( \frac{\omega}{\delta} \right) + H_b(\omega) - \frac{\log A_{\omega n}}{n} + G(\omega) \right| \]
\[ \leq \sup_{\delta \in [a,1]} \sup_{\omega \in [0,\delta]} \left| \frac{1}{n} \log \frac{q - 1}{\delta(n + 1)} + \sup_{\omega \in [0,\delta]} \left| \frac{\log A_{\omega n}}{n} - G(\omega) \right| \right| \]
where ‘a’ is due to Lemma 2 and ‘b’ to triangle inequality. In the last expression, the first addend converges to zero as $n \to \infty$ since $q$ is constant and $\delta \in [a, 1]$ with $a > 0$. Moreover, the second addend converges to zero due to the hypothesis that $(1/n) \log A_{\omega n} \to G(\omega)$ and by Lemma 1. Again by Lemma 1 we conclude that $g_{\delta,n}(\delta) \Rightarrow g(\delta)$.

Uniform convergence of $g_{\delta,n}(\delta)$ to $g(\delta)$ turns into uniform convergence of $g_{\delta,n}^+(\delta)$ to $g^+(\delta)$. In fact, we have $|g_{\delta,n}^+(\delta) - g^+(\delta)| \leq |g_{\delta,n}(\delta) - g(\delta)|$ for all $\delta$ and $n$, which implies
\[ 0 \leq \left| g_{\delta,n}^+(\delta) - g^+(\delta) \right| \leq \sup_{\delta \in [a,1]} g_{\delta,n}(\delta) - g(\delta). \]

By squeeze theorem we have $\sup_{\delta \in [a,1]} |g_{\delta,n}^+(\delta) - g^+(\delta)| \to 0$ as $n \to \infty$, and therefore $g_{\delta,n}^+ \Rightarrow g^+$ by Lemma 1.

We are now in a position to prove uniform convergence of $f_{\epsilon,n}$ to $f_\epsilon$. In fact, we have
\[ \sup_{\delta \in [a,1]} \left| f_{\epsilon,n}(\delta) - f_\epsilon(\delta) \right| = \sup_{\delta \in [a,1]} \left| - \frac{\log n}{n} + g_{\delta,n}^+(\delta) - g^+(\delta) \right| \]
\[ \leq \left| \frac{\log n}{n} \right| + \sup_{\delta \in [a,1]} \left| g_{\delta,n}^+(\delta) - g^+(\delta) \right| \]
where we applied triangle inequality. Convergence to zero of the last expression is guaranteed by $g_{\delta,n}^+ \Rightarrow g^+$.

Uniform convergence of $f_{\epsilon,n}(\delta)$ to $f_\epsilon(\delta)$ leads us to the statement, as follows. Recall that, if $f_n \Rightarrow f$ on $A_0$ then
\[ \lim_{n \to \infty} \inf_{x \in A_n} f_n(x) = \inf_{x \in A_0} \lim_{n \to \infty} f_n(x) = \inf_{x \in A_0} f(x), \]
i.e., we can exchange limit and infimum. Hence we can write
\[ \lim_{n \to \infty} - \frac{1}{n} \log \mathbb{E}_{C(n,r,q)}[P_B(C, \epsilon)] \geq \inf_{\delta \in (0,1)} f_{\epsilon,n}(\delta) \]
\[ = \inf_{\delta \in (0,1)} f_\epsilon(\delta). \]

In the previous equation array, the first inequality is justified by the fact that if $\alpha_n \to \alpha, \beta_n \to \beta$, and $\alpha_n \geq \beta_n$ for all $n$ (possibly, larger than some $n_0$), then $\alpha \geq \beta$. Moreover, the two equalities are justified by $f_{\epsilon,n}(\delta) \Rightarrow f_\epsilon(\delta)$.

**Remark 1.** The function $E_C(\epsilon)$ given by (3) is nonnegative for all $0 < \epsilon < 1$, since it is defined as the infimum of the sum of two nonnegative quantities. Moreover, since $E_C(\epsilon)$ bounds the error exponent of the given ensemble from below, it must fulfill $E_C(\epsilon) = 0$ for all $1 - r \leq \epsilon \leq 1$.

**Remark 2.** The lower bound $E_G(\epsilon)$ turns out to be useless for all ensembles for which $G(\omega) \to 0$ as $\omega \to 0^+$, as for any such ensemble we have $E_G(\epsilon) = 0$ for all $0 < \epsilon < 1$.

To see this, simply observe that under this setting we have $\inf_{\omega \in [0,\delta]} h_{\delta}(\omega) \leq \lim_{\omega \to 0^+} h_{\delta}(\omega) = 0$ for all $0 < \delta \leq 1$, and therefore $g^+(\delta) = 0$ for all $0 < \delta \leq 1$. Then, $E_G(\epsilon) = \inf_{\delta \in (0,1]} D(\delta, \epsilon) = 0$ for all $0 < \epsilon < 1$ (simply take $\delta = \epsilon$).

The following lemma, whose proof is available in [11], characterizes the function $g^+(\delta)$ defined in (4).

**Lemma 3.** The function $g^+(\delta)$ has the following properties:
1) $g^+(\delta) = 0$ for all $1 - r \leq \delta \leq 1$;
2) If $G(\omega)$ is continuous in $(0, 1)$ then $g^+(\delta)$ is non-increasing and continuous;
3) If $G(\omega)$ is continuous in $(0, 1)$ and $\lim_{\omega \to 0^+} G(\omega) = \gamma > 0$ then:
   a) $\lim_{\omega \to 0^+} g^+(\delta) = |\gamma|$;
   b) $\delta^* = \sup \{ \delta \in [0, 1 - r] : g^+(\delta) > 0 \}$ is strictly positive;
   c) $g^+(\delta) > 0 \forall \delta \in (0, \delta^*)$: $g^+(\delta) = 0 \forall \delta \in [\delta^*, 1]$.

The next theorem, whose proof is again available in [11], shows that, under conditions on $G(\omega)$, there exists an interval of values of $\epsilon$ over which $E_G(\epsilon)$ is positive. For the corresponding ensembles, $E_G(\epsilon)$ is therefore useful to lower bound $c^*_{ML}$.

**Theorem 2.** Let $\delta^* = \sup \{ \delta \in [0, 1 - r] : g^+(\delta) > 0 \} \leq 1 - r$.
If $G(\omega)$ is continuous in $(0, 1)$ and $\lim_{\omega \to 0^+} G(\omega) < \gamma$, then $E_G(\epsilon) > 0 \forall \epsilon \in (0, \delta^*)$ and $E_G(\epsilon) = 0 \forall \epsilon \in [\delta^*, 1]$, and therefore $c^*_{ML} \geq \delta^*$. In the next section we present results for two ensembles fulfilling the hypotheses of Theorem 2, namely, the ensemble of linear random parity-check codes over $\mathbb{F}_q$ and the ensemble
of fixed-rate binary Raptor codes with linear random precoders [9]. For the first ensemble the function \( E_G(\epsilon) \) can be obtained analytically and coincides with Gallager’s random coding bound over the \( q \)-EC. For the second one, \( E_G(\epsilon) \) shall be computed numerically. However, if only the lower bound on \( \epsilon_{\text{ML}}^* \) is of interest, it may be computed by simply solving a \( 2 \times 2 \) system of equations.

IV. Results for Specific Ensembles

A. Linear Random Parity-Check Codes

Consider the ensemble of linear random parity-check codes over \( \mathbb{F}_q \) induced by an \((1-r)n \times n\) random parity-check matrix whose entries are independent and identically distributed (i.i.d.) random variables uniformly distributed in \( \mathbb{F}_q \). For this ensemble we have the following result.

**Theorem 3.** For the ensemble of linear random parity-check codes we have \( \delta^* = 1-r \) and therefore \( \epsilon_{\text{ML}}^* = 1-r \). Moreover

\[
E_G(\epsilon) = \begin{cases} 
-\log \left( \frac{1-\epsilon}{q} + \epsilon \right) - r \log q & 0 < \epsilon < \epsilon_c \\
D(1-r,\epsilon) & \epsilon_c \leq \epsilon < 1-r \\
0 & \epsilon \geq 1-r
\end{cases}
\]

(9)

where \( \epsilon_c = (1-r)/(1+(q-1)r) \).

**Proof:** The expected weight enumerator of the linear random parity-check ensemble is \( A_{\omega,n} = \binom{n}{\omega} \omega^q \) and the corresponding weight spectral shape is \( G(\omega) = H_b(\omega) + \omega \log(q-1) - (1-r) \log q \). Uniform convergence of \( \frac{1}{n} \log A_{\omega,n} \) to \( G(\omega) \) may be proved in a very simple way, by observing that

\[
\sup_{\omega} \left| \frac{1}{n} \log A_{\omega,n} - G(\omega) \right| = \sup_{\omega} \left| \frac{1}{n} \log \left( \binom{n}{\omega} \omega^q \right) - H_b(\omega) \right| \\
\leq \sup_{\omega} \left| \frac{\log(n+1)}{n} \right| = \left| \frac{\log(n+1)}{n} \right|
\]

where we applied the lower bound in (2). Since \( \lim_{n \to \infty} \frac{\log(n+1)}{n} = 0 \) as \( n \to \infty, \) we conclude that \( \frac{1}{n} \log A_{\omega,n} \to G(\omega) \).

The function \( h_\delta(\omega) \) defined in (8) assumes the form

\[
h_\delta(\omega) = -\delta H_b \left( \frac{\omega}{\delta} \right) - \omega \log(q-1) + (1-r) \log q.
\]

Let \( \hat{\omega}(\delta) = \frac{2-1}{q} \delta \). It is easy to see that this function tends to \((1-r) \log q\) when \( \omega \to 0^+ \), is monotonically decreasing for \( \omega \in (0,\hat{\omega}(\delta)) \), takes a minimum at \( \omega = \hat{\omega}(\delta) \), and increases monotonically for \( \omega \in (\hat{\omega}(\delta),\delta) \). Hence, we have \( g(\omega) = \inf_{\omega \in (0,\delta)} h_\delta(\omega) = h_\delta(\hat{\omega}(\delta)) = (1-r-\delta) \log q \) so that

\[
g^+(\delta) = \max \{ 0, g(\delta) \} = \begin{cases} 
(1-r-\delta) \log q & \text{if } 0 < \delta < 1-r \\
0 & \text{if } 1-r \leq \delta < 1.
\end{cases}
\]

The parameter \( \delta^* = 1-r \) and \( \epsilon_{\text{ML}}^* \leq 1-r \). Next, we develop \( E_G(\epsilon) \) analytically. Based on the above findings, we have

\[
E_G(\epsilon) = \min \left\{ \inf_{\delta \in (0,1-r)} \left[ D(\delta, \epsilon) + (1-r-\delta) \log q \right], \inf_{\delta \in [1-r,1]} D(\delta, \epsilon) \right\}
\]

that immediately yields \( E_G(\epsilon) = 0 \) for all \( \epsilon \geq 1-r \) (it suffices to take \( \delta = \epsilon \), corresponding to the third row of (9)). For \( 0 < \epsilon < 1-r \) we need to analyze the function \( f_\epsilon(\delta) = D(\delta, \epsilon) + g^+(\delta) = D(\delta, \epsilon) + (1-r-\delta) \log q \). Let \( \delta(\epsilon) = \frac{q}{(q-1)^2} \).

Taking the derivative with respect to \( \delta \), it is immediate to see that this function decreases monotonically for \( \delta \leq \delta(\epsilon) \), takes a minimum at \( \delta = \delta(\epsilon) \), and increases monotonically for \( \delta > \delta(\epsilon) \). Hereafter we need to distinguish the two cases \( \delta(\epsilon) < 1-r \) and \( \delta(\epsilon) \geq 1-r \). It is immediate to verify that they correspond to \( 0 < \epsilon < \epsilon_c \) and \( \epsilon_c \leq \epsilon < 1-r \), respectively, where \( \epsilon_c = (1-r)/(1+(q-1)r) \).

**Case 1:** \( 0 < \epsilon < \epsilon_c \). In this case the function \( D(\delta, \epsilon) + (1-r-\delta) \log q \) has a minimum at \( \delta = \delta(\epsilon) \). It takes the value \( D(1-r, \epsilon) \) at \( \delta = 1-r \). Therefore we obtain

\[
E_G(\epsilon) = \min \left\{ D(\delta(\epsilon), \epsilon) + (1-r-\delta(\epsilon)) \log q, D(1-r, \epsilon) \right\}
\]

\[
= D(\delta(\epsilon), \epsilon) + (1-r-\delta(\epsilon)) \log q
\]

\[
= -\log \left( \frac{1-\epsilon}{q} + \epsilon \right) - r \log q
\]

where the third expression follows from simple algebraic manipulation. This yields the first row of (9).

**Case 2:** \( \epsilon_c < \epsilon < 1-r \). In this case the function \( D(\delta, \epsilon) + (1-r-\delta) \log q \) is monotonically decreasing for \( \delta \in (0,1-r) \), so its infimum is taken as \( \delta \to (1-r)^- \). We obtain \( E_G(\epsilon) = \min \{ D(1-r, \epsilon), D(1-r, \epsilon) \} \) that corresponds to the second row of (9).

**Remark 3.** Interestingly, the expression (9) of \( E_G(\epsilon) \) turns out to coincide with that of Gallager’s random coding error exponent for the \( q \)-EC [12].

B. Fixed-Rate Raptor Codes with Linear Random Precoders

In this subsection we consider binary fixed-rate Raptor code ensembles with linear random precoding. A vector of \( r_n \) information bits is first encoded by an outer linear block code picked randomly in the ensemble of binary linear random parity-check codes with design rate \( r_o \), providing a vector of \( r_n/r_o \) intermediate bits. Intermediate bits are further encoded by an inner fixed-rate Luby-transform (LT) code of rate \( r \) and output degree distribution \( B(\nu) = \sum_j \nu_j x^j \), generating \( n \) encoded bits. The overall design rate is \( r = r_o r \).

The weight spectral shape of this ensemble was characterized in [9]. It is given by

\[
G(\omega) = H_b(\omega) - r_i(1-r_o) - \nu_\omega(\lambda_0)
\]

(10)

where

\[
\nu_\omega(\lambda) = H_b(\lambda) + \omega \log(\rho(\lambda)) + (1-\omega) \log(1-\rho(\lambda))
\]

(11)

and

\[
\lambda_0 = \lambda_0(\omega) = \arg\max_{\lambda \in \mathcal{D}} \nu_\omega(\lambda).
\]

In (11), \( \mathcal{D} = [0,1] \) if \( \Omega_j = 0 \) for any even \( j \) and \( \mathcal{D} = (0,1] \) otherwise. Moreover, \( \rho(\lambda) = \frac{1}{2} \sum_{i=1}^d \Omega_j[1-(1-2\lambda)^j] \), being \( d \) the maximum LT output degree. Again from [9]:

1) \( G(\omega) \) in (10) is continuous.
2) \( \lim_{\omega \to 0^+} G(\omega) < 0 \) iff \((r_i, r_o) \in \mathcal{P}\), where
\[
\mathcal{P} = \left\{ (r_i, r_o) \geq (0,0) : r_i(1 - r_o) > \max_{\lambda \in \mathcal{D}} \left[ r_i H_b(\lambda) + \log(1 - \rho(\lambda)) \right] \right\}.
\] (12)

3) The derivative of \( G(\omega) \) is
\[
G'(\omega) = \log \frac{1 - \omega}{\omega} + \log \frac{\rho(\lambda_0)}{1 - \rho(\lambda_0)}.
\] (13)

4) \( G'(\omega) > 0 \) for \( 0 < \omega < \frac{1}{2} \) and \( \lim_{\omega \to 0^+} G'(\omega) = +\infty \).

Uniform convergence of \( \frac{1}{n} \log A_n \) to \( G(\omega) \) can be proved using arguments from [9, Sec. III]. Moreover, the hypotheses of Theorem 2 are satisfied when \((r_i, r_o) \in \mathcal{P}\), where \( \mathcal{P} \) is given by (12). As opposed to linear random parity-check ensembles, in this case \( E_G(e) \) shall be computed numerically. However, if only the lower bound \( \delta^* \) on the ML decoding threshold \( \epsilon_{\text{ML}} \) is of interest, it may be computed efficiently, as shown next.

**Theorem 4.** Consider a binary Raptor ensemble over a channel with linear random precoder and let \((r_i, r_o) \in \mathcal{P}\). Then \( \epsilon_{\text{ML}} \geq \delta^* \) where \( \delta^* \) is the smallest \( \delta \) s.t. \((\hat{\delta}, \lambda_0)\) is a solution of the \( 2 \times 2 \) system
\[
r_i(1 - r_o) - r_i H_b(\lambda_0) - (1 - \hat{\delta}) \log(1 - \rho(\lambda_0)) = 0
\]
\[
r_i \log \frac{1 - \hat{\lambda}_0}{\lambda_0} - \frac{1 - \hat{\delta}}{1 - \rho(\lambda_0)} \rho(\hat{\lambda}_0) \log e = 0.
\] (14)

**Proof:** If \((r_i, r_o) \in \mathcal{P}\) then Theorem 2 applies. We have \( \epsilon_{\text{ML}} \geq \delta^* \), where \( \delta^* = \sup_{\delta} \{ \delta \in [0,1 - r_i] : g^+(\delta) > 0 \} \) and \( \delta^* > 0 \). Owing to continuity of \( h_3(\omega) \) we can write \( g^+(\delta) = \max\{0, h_3(\hat{\omega})\} \), where \( \hat{\omega} = \hat{\omega}(\hat{\delta}) = \arg \max_{\omega \in (0,\delta]} h_3(\omega) \).

From (8) and (13) we obtain
\[
\frac{d h_3(\omega)}{d \omega} = \log \frac{\omega}{\delta - \omega} - \log \frac{\rho(\lambda_0)}{1 - \rho(\lambda_0)}
\] (16)
which reveals how \( d h_3(\omega)/d \omega \to +\infty \) as \( \omega \to \delta^* \). Thus, the maximum cannot be taken at \( \omega = \delta \) and \( \hat{\omega} \) must be a solution of \( d h_3(\omega)/d \omega = 0 \). Defining \( \lambda_0 = \arg \max_{\lambda \in \Omega(\lambda)} \mu_{\omega}(\lambda) \) and recalling (16), after some algebraic manipulation this translates to
\[
\hat{\omega} = \delta \rho(\hat{\lambda}_0)
\] (17)

The parameter \( \lambda_0 \) must be a solution of \( d \mu_{\omega}(\lambda)/d \lambda = 0 \). Developing the derivative we obtain
\[
r_i \log \frac{1 - \hat{\lambda}_0}{\lambda_0} + \hat{\omega} \frac{\rho'(\hat{\lambda}_0)}{\rho(\hat{\lambda}_0)} \log e - (1 - \hat{\omega}) \frac{\rho'(\hat{\lambda}_0)}{1 - \rho(\hat{\lambda}_0)} \log e = 0.
\] (18)

So far we have shown that \( g^+(\delta) = \max\{0, h_3(\hat{\omega})\} \) where \( (\hat{\omega}, \hat{\lambda}_0) \) is a solution of the system of simultaneous equations (17) and (18). Recall now from Theorem 2 that \( g^+(\delta) > 0 \) for all \( 0 < \delta < \delta^* \) and \( g^+(\delta) = 0 \) for all \( \delta^* \leq \delta \leq 1 \). This necessarily implies \( h_3(\hat{\omega}) > 0 \) for all \( 0 < \delta < \delta^* \) and

\[\rho(\lambda_0(\omega))\] cannot converge to \( 1 \) as \( \omega \to \delta^* \) for any \( 0 < \delta^* < 1 - r_i \).