Fixed-energy random coding with rescaled codewords at the transmitter

Author(s):
Fehr, Daniel; Scarlett, Jonathan; Martinez, Alfonso

Publication Date:
2016

Permalink:
https://doi.org/10.3929/ethz-a-010645960

Rights / License:
In Copyright - Non-Commercial Use Permitted
Fixed-Energy Random Coding with Rescaled Codewords at the Transmitter

Daniel Fehr∗, Jonathan Scarlett † and Alfonso Martinez∗
∗Universitat Pompeu Fabra, Barcelona
†École Polytechnique Fédérale de Lausanne

e-mail: daniel.co@bluewin.ch, jmscarlett@gmail.com, alfonso.martinez@ieee.org

Abstract—This paper proposes a new method to reduce the error rate of channel codes over an AWGN channel by renormalizing the codewords to a constant energy before transmission and decoding with the original codebook. Evaluation of the random-coding error exponent reveals that this normalization technique approaches the constant-composition error exponent for certain pairs of rate and signal-to-noise ratio.

I. INTRODUCTION

Given a general coded modulation scheme over an AWGN channel, we investigate the effect on the error rate of rescaling the transmitted codewords so that their energy is constant. We compare the proposed technique with the standard coded decoding with the original codebook. Evaluation of the random-coding error exponent reveals that this normalization technique approaches the constant-composition error exponent for certain pairs of rate and signal-to-noise ratio.

II. MODEL

The channel input sequence \( x = (x_1, \ldots, x_n) \) consists of \( n \) symbols \( x \in \mathcal{X} \), where \( \mathcal{X} \) is the symbol constellation. We denote the channel output sequence by \( y \) and the channel law, that is, the conditional probability density of receiving sequence \( y \) when the sequence \( x \) has been sent, by \( W^n(y \mid x) \). We represent random variables by capital letters and their realizations by lowercase letters, e.g., \( X = (X_1, \ldots, X_n) \) and \( Y = (Y_1, \ldots, Y_n) \) denote random input and output vectors. The channel is memoryless and \( W^n(y \mid x) = \prod_{i=1}^{n} W(y_i \mid x_i) \), where \( W(y \mid x) \) is the single-letter channel law.

We focus on a complex-valued additive white Gaussian noise (AWGN) channel. The input alphabet \( \mathcal{X} \) is a finite subset of the complex numbers and the channel output is given by

\[
y_i = \sqrt{\text{SNR}} x_i + z_i, \quad i = 1, \ldots, n
\]

where \( x_i \) are the symbols, \( y_i \) the channel output values and SNR is the signal-to-noise ratio. The noise values \( z_i \) are drawn from a circularly-symmetric complex-valued Gaussian random variable with zero mean and unit variance. Therefore, the symbol channel transition probability is given by

\[
W(y \mid x) = \frac{1}{\pi} e^{-|y - \sqrt{\text{SNR}} x|^2}.
\]

The empirical average symbol energy of channel input sequence \( x \) is \( \mathbb{E}[E(x)] = \frac{1}{n} \sum_{i=1}^{n} |x_i|^2 \). Let \( Q \) be a distribution on the symbols in \( \mathcal{X} \). We require that the constellation \( \mathcal{X} \) is chosen such that the identities \( \mathbb{E}[X] = 0 \) and \( \mathbb{E}[|X|^2] = 1 \) hold, where the expectations are with respect to \( Q \).

We use \( \mathcal{P}[A] \) to denote the probability of an event \( A \), and \( \mathbb{E}[\cdot] \) is the expectation operator. We denote the Kullback-Leibler Divergence as \( D(P \| Q) \), the set of all compositions on length-\( n \) sequences drawn from \( \mathcal{X} \) as \( \mathcal{P}_n \), the set of all distributions on \( \mathcal{X} \) as \( \mathcal{P} \) and the image of set \( A \) under the function \( f \) as \( f[A] \).

We denote the channel code by \( C_n \). The code consists of \( M \) codewords \( x \), i.e., \( C_n = \{x^{(1)}, \ldots, x^{(M)}\} \), and the corresponding code is said to be an \( (n, M) \) block code of block length \( n \). The encoder assigns to each message \( m \in \{1, \ldots, M\} \) a codeword \( x^{(m)} \) from the codebook \( C_n \). We assume that the message \( m \) is drawn according to a uniform distribution. The rate of a code is defined as \( R = \frac{\log_2 M}{n} \).

The decoder outputs an estimated message \( \hat{m} \) according to a maximum-likelihood rule

\[
\hat{m} = \arg \max_{m \in M} q^n(x^{(i)}, y),
\]

where \( q^n \) denotes the metric that the decoder uses to estimate which message \( m \) has been sent. We focus on metrics \( q^n \) that can be expressed in terms of the letter metric \( q \) as in

\[
q^n(x, y) = \prod_{i=1}^{n} q(x_i, y_i).
\]

Further, we require \( q \) to be positive.

An error occurs if the decoder’s estimate differs from the sent message, i.e. \( \hat{m} \neq m \). The error probability of a code \( C_n \) is

\[
p_e(C_n) = \frac{1}{M} \sum_{m \in M} p_e(m, C_n)
\]

and we equivalently write

\[
p_e(n, M) = p_e(C_n).
\]

Finally, an error exponent \( E(Q, R) \) is
said to be achievable if there exists a sequence of \((n,M)\)-codes \(C_n\) such that
\[
\liminf_{n \to \infty} \frac{1}{n} \log p_e(C_n) \geq E(Q,R).
\] (4)

III. CODEWORD RESCALING

A. Rescaling setup

Let a rescaler \(\eta\) be a block that performs the operation
\[
\eta(x) = \mathcal{E}(x)^{-\frac{1}{2}} x
\] (5)
on a codeword \(x\); that is, it renormalizes the codeword \(x\) such that the empirical codeword energy is \(\mathcal{E}(\eta(x)) = 1\).

We consider a coded modulation scheme that consists of an encoder and a rescaler \(\eta\). The encoder maps message \(m\) into codeword \(x^{(m)} = \phi(m)\) using codebook \(C\), the rescaler outputs an energy-normalized version \(\tilde{x}^{(m)}\) of the codeword \(x^{(m)}\). The rescaling operation can be thought of as part of the encoder’s codebook, so that we use a code \(\tilde{C}\) with rescaled codewords \(\tilde{x}\) that consist of symbols \(\tilde{x}\) from an expanded constellation \(\mathcal{X}\).

The decoder outputs the estimate \(\hat{m}\) under the original codebook \(C\) by maximizing the metric \(\rho^s\). With the choice of \(q^n(x, y) = W^n(y|x)\), we have an instance of mismatched decoding, since the decoder does not account for the rescaling operation neither in the codebook \(C\) nor in the decoding metric. We consider a slightly more general choice given by \(q^n(x, y) = W^n(y|\beta x)\), where \(\beta\) may be optimized to minimize the error probability; however, it cannot depend on the codeword, and hence it cannot be used to undo the rescaling. Note that for a practical code, \(\beta\) is fixed before deployment and such a decoding metric can be implemented without additional computational complexity.

We can build an equivalent model for the rescaling setup by removing the rescaling block from the transmitter and reintroducing it as a channel property. With this model, the scaling function leads to a new channel law
\[
\tilde{W}^n(y|x) = W^n(y|\eta(x)).
\] (6)

Note that \(\tilde{W}^n\) does not represent a memoryless channel.

B. Scaling exponent

We study the i.i.d. random-coding error probability. We consider an ensemble of codebooks with block length \(n\) and \(M = 2^{nR}\) codewords. The ensemble consists of codebooks whose codewords \(x^{(i)}, i = 1, \ldots, M\) are randomly generated. A codeword \(x^{(i)} = (x_1, \ldots, x_n)\) at entry \(i\) in the random codebook is generated by drawing its \(n\) symbols according to the distribution \(Q(X)\). We are interested in the achievable random-coding exponent \(E^{\text{sc}1}(Q,R)\) of the ensemble average of the error probability \(\rho_{\text{sc}}(n,M) = \sum_{x} p(C_n|p_e(C_n))\).

Theorem 1 (Scaling random-coding exponent): The random-coding error probability in a rescaling setup satisfies
\[
\lim_{n \to \infty} \frac{1}{n} \log_2 \rho_{\text{sc}}(n,2^{nR}) \geq E^{\text{sc}1}(Q,R),
\] (7)
where the scaling exponent is defined as
\[
E^{\text{sc}1,\beta}(Q,R) \triangleq \sup_{\rho \geq 0} \sup_{p_e \in \mathcal{P}(n)} \left\{ E^{\text{sc}1}(Q,\rho, s(P)) - \rho R \right\},
\] (8)
and the corresponding \(E^{\text{sc}1,\beta}_0\) is defined as
\[
E^{\text{sc}1,\beta}_0(Q,\rho, s(P)) \triangleq D(P\|Q) - \mathbb{E} \left[ \log_2 \mathbb{E} \left[ \frac{q^n(x,\tilde{X})^s(x,\tilde{Y})}{q^n(x,\tilde{Y})^{\rho s}} \mid X \right] \right],
\] (9)

and the expectations are with respect to
\[
(X, Y, \tilde{X}) \sim P(x) W(y|\mathcal{E}(x)^{-\frac{1}{2}} x) Q^n(\tilde{x}).
\] (10)

Proof: For the ensemble of codebooks with \(M\) codewords of length \(n\), chosen according to random-coding distribution \(Q^n\), transmitted over a channel described by the arbitrary channel law \(W^n\) and decoded according to the metric \(\rho^n\), the average ensemble error probability is bounded by the random-coding union (RCU) bound [4, 5]
\[
\rho_{\text{rcu}}(n,M) \leq \mathbb{E} \left[ \min \left\{ 1, (M - 1) \mathbb{P} \left[ q^n(\tilde{X},Y) \geq q^n(X,Y) \mid X,Y \right] \right\} \right],
\] (11)
where \((X, Y, \tilde{X}) \sim Q^n(x) W^n(y|x) Q^n(\tilde{x})\).

Weakening (11) by replacing the function \(z \mapsto \min\{1, z\}\) with the function \(z \mapsto z^{(\rho(x))}\) and using Markov’s inequality with parameter \(s(x)\), leads to the definition of a parametrized upper bound on the the RCU bound
\[
\rho_{\text{rcu},s}(n,M) \triangleq \mathbb{E} \left[ \left( \mathbb{E} \left[ q^n(x,\tilde{X})^{s(X)} / q^n(x,\tilde{Y})^{\rho(X)} \mid X \right] \right)^{-1} \right],
\] (12)
that holds for all pairs of functions \((\rho(x), s(x))\) such that \(\rho(X^n) \leq [0,1]\) and \(s(X^n) \leq [0, \infty]\).

We further weaken (12) by applying \(M - 1 \leq 2^{nR}\), use the random-coding distribution \(Q^n_{\text{id}} = \prod_{i=1}^n Q(x_i)\) and the equivalent scaling channel model (6), to obtain
\[
\rho_{\text{sc}}(n,M) \leq \sum_{x \in \mathcal{X}^n} 2^{n(\rho(x) R)} Q^n_{\text{id}}(x) f^n(\rho(x), s(x), x),
\] (13)
where
\[
f^n(\rho, s, x) \triangleq \int_x W(y \mid \mathcal{E}(x)^{-\frac{1}{2}} x) \left( \sum_{\tilde{x} \in \mathcal{X}^n} Q^n_{\text{id}}(\tilde{x}) q^n(\tilde{x},y)^s q^n(x,y)^s \right)^{\rho} dy.
\] (14)

We split the outer summation over the channel-input sequences in (13) into summations over sequences \(x\) of composition \(P = \tilde{P}\) and obtain
\[
\rho_{\text{sc}}(n,M) \leq \sum_{P \in \mathcal{P}} 2^{n(\rho(P) R)} \sum_{x \in \mathcal{T}(P)} Q^n_{\text{id}}(x) f^n(\rho(P), s(P), x),
\] (15)
We also reduced the degrees of freedom for the parameters \( \rho(x) \) and \( s(x) \) such that they only depend on the composition \( P = P_x \). This simplifies the analysis.

The codeword average symbol energy only depends on the codewords composition. Hence we write \( E(x) = E(P_x) \) and use it in (14) to obtain \( f^n(\rho, s, P, x) \). This, together with the product nature of decoding metric, channel law and \( Q_{\text{bound}}^n \), allows us to factor \( f^n \) as \( f^n(\rho, s, P, x) = \prod_{i=1}^{n,M} f(\rho, s, P, x_i) \), where

\[
f(\rho, s, P, x) \triangleq \int W(y | E(P))^{-\frac{1}{2}} x y \left( \sum_{\lambda \in \mathcal{X}} Q(\lambda)^{q(x,y)} \frac{q(x,y)^{\rho}}{q(x,y)^{\rho}} d y \right),
\]

(16)

by invoking the distributive law. For the product in \( f^n \), only the composition of \( x \) is relevant, that is, it can be expressed independent of \( x \) as \( f^n(\rho, s, P) = \prod_{x \in \mathcal{X}} f(\rho, s, P, x)^{a(P, x)} \).

We use this form in (15) to obtain

\[
\mathcal{P}(n, M) \leq \sum_{P \in \mathcal{P}_n} \sum_{x \in \mathcal{T}(P)} 2^{nQ(\rho, s, P, x)} f(\rho, s, P, x)^{a(P, x)},
\]

(17)

where we expressed the codeword probability in terms of its composition as in \( Q_{\text{bound}}^n(\mathcal{X}) = 2^{-n(D(\mathcal{P}_n) + H(P_n))} \).

Since the summand is independent of the code word \( x \) in (17), we can upper-bound the summation over the codewords by using the bound on the number of sequences in a composition class \( |T(P)| \leq 2^{nH(P)} \). Doing some rearrangements and bringing all terms on a common exponent base, we obtain

\[
\mathcal{P}(n, M) \leq \sum_{P \in \mathcal{P}_n} 2^{-nQ(\rho, s, P, x)} f(\rho, s, P, x)^{a(P, x)},
\]

(18)

where

\[
\xi(\rho, s, P, R) \triangleq D(P||Q) - \sum_{x \in \mathcal{X}} P(x) \log f(\rho, s, P, x) - \rho R.
\]

(19)

A simple upper bound on a sum is obtained by fixing its summands to the largest one, that is \( n_{\max} \leq |\mathcal{X}| \). We weaken (18) with this bound and the fact that the number of compositions is bounded by \( |P_n| \leq (n + 1)^{|\mathcal{X}|} \) and get

\[
\mathcal{P}(n, M) \leq (n + 1)^{|\mathcal{X}|} 2^{-n \min_{P \in \mathcal{P}_n} \xi(\rho, s, P, x)}.
\]

(20)

The bound (20) is achievable for any pair of parameters \((\rho(P), s(P))\), which we exploit by choosing them such that the bound gets as tight as possible. By definition of the min and sup operators, this is the case when we replace \( \xi \) with

\[
\xi^*(P, R) = \sup_{0 \leq \rho \leq 1, s \geq 0} \xi(\rho, s, P, R).
\]

(21)

That is, place the supremum inside the minimum operator.

Finally, we observe the sub-exponential factor in (20) which suggests to transform the inequality as

\[
-\frac{1}{n} \log_2 \mathcal{P}(n, 2^n R) \geq \min_{P \in \mathcal{P}_n} \xi^*(P, R) - |\mathcal{X}| \log_2 (n + 1)
\]

(22)

and take the limit

\[
\lim_{n \to \infty} -\frac{1}{n} \log_2 \mathcal{P}(n, 2^n R) \geq \min_{P \in \mathcal{P}_n} \xi^*(P, R).
\]

(23)

\begin{equation}
\begin{aligned}
\text{C. Swapped exponent}
\end{aligned}
\end{equation}

An inspection by example of the optimization parameters in (8) shows that \( E_0^{\text{swp}}(Q, R) \) is not convex in \( P \) for fixed values of \( \rho, s \) and \( R \), which complicates its numerical computation. Further, note that it is crucial to find the true \( P^* \) to guarantee the achievability of \( E_0^{\text{swp}}(Q, R) \), since \( P^* \) is the result of a minimization over a variable that is not an arbitrary parameter. For these reasons, we introduce a lower bound on (8) that is computationally tractable.

\textbf{Theorem 2 (Swapped scaling random-coding exponent):} The swapped random-coding error exponent, defined as

\[
E_0^{\text{swp}}(Q, R) \triangleq \sup_{\beta > 0, \epsilon > \epsilon_0} \sup_{\rho \in [0, 1]} \{ E_0^{\text{swp}}(Q, \rho, s, \epsilon) - \rho R \}
\]

with

\[
E_0^{\text{swp}}(Q, \rho, s, \epsilon) \triangleq \min_{P \in \mathcal{P}_s} \left\{ D(P||Q) - \epsilon \log_2 \mathbf{E} \left[ \log_2 \mathbf{E} \left[ q(x, y)^{P(x)} \right] | Y \right] \mathbf{E} X \right\}
\]

(24)

is a lower bound on \( E_0^{\text{swp}}(Q, R) \), where \( \epsilon \) is optimized over the interval \( S = [\min_{x \in \mathcal{X}} |x|^{\rho}, \max_{x \in \mathcal{X}} |x|^{\rho}] \), the set \( \mathcal{P}_s \) is \( \{ P \in \mathcal{P} | E(P) = \epsilon \} \) and the expectations are according to \( (X, Y, X) \sim (P(x)W(y | c^{-\frac{1}{2}} x)Q(x)) \).

\textbf{Proof:} First, let the energy level \( \epsilon \) denote the expected symbol energy with respect to \( P \) or equivalently \( \epsilon = E(P) \). We observe that the probability simplex \( \mathcal{P} \) can be partitioned into disjoint subsets \( \mathcal{P}_s \), where a subset consists of all distributions \( P \) that obtain the energy level \( \epsilon \), that is, we have \( \mathcal{P} = \bigcup_{s \in S} \mathcal{P}_s \) where \( \mathcal{P}_s = \{ P \in \mathcal{P} | E(P) = \epsilon \} \) and \( S = [\min_{x \in \mathcal{X}} |x|^{\rho}, \max_{x \in \mathcal{X}} |x|^{\rho}] \). The subsets \( \mathcal{P}_s \) are compact and convex since they are intersections of two hyperplanes and the closed positive orthant [7]. In correspondence with these observations, we rephrase the scaling exponent (8) in terms of energy levels and subsets as

\[
E_0^{\text{swp}}(Q, R) = \min_{s \in S} \sup_{\rho \in [0, 1]} \{ E_0^{\text{swp}}(Q, \rho, s, P) - \rho R \}.
\]

(26)

We swap the order of the inner two optimization operators and define \( E_0^{\text{swp}}(Q, R) \) and \( E_0^{\text{swp}}(Q) \) as in (24) and (25) respectively. Observing that the minimax inequality

\[
\sup_{x, y} \min_{x, y} f(x, y) \leq \min_{x, y} \sup_{x, y} f(x, y)
\]

(27)

holds we conclude that swapping the order of optimization results in a lower bound on (8).
IV. Numerical Results

We are interested in how the error exponent of channel-coding with rescaling performs with respect to setups with the iid and constant-composition exponents \cite{1}, \cite{2}.

For a discrete-input continuous-output memoryless channel with ML decoder and input distribution $Q$, the iid exponent is given by \cite{1}

$$E_{cr}^{(i)}(Q, R) = \max_{\rho \in [0,1]} E_{cr}^{(i)}(\rho) - \rho R,$$

where

$$E_{cr}^{(i)}(Q, \rho) = -\log_2 \int_E W(y|X) E_i(y|\rho) \, dy$$

is the Gallager function \cite{3}. The expectation is taken with respect to $Q$.

For a discrete-input continuous-output memoryless channel with ML decoder and input distribution $Q$, the constant-composition exponent is given by \cite{1}

$$E_{cc}^{(c)}(Q, R) = \max_{\rho \in [0,1]} E_{cc}^{(c)}(\rho) - \rho R,$$

where

$$E_{cc}^{(c)}(Q, \rho) = -\log_2 \int_{X|Y} E_{Q} \left[ W(y|X) \right] \left(1+\rho \right) \, dy$$

and $\phi_{a} = E_{Q}[a(X)]$, and the optimization in (31) is over all real-valued functions $a$. The expectations are taken with respect to $(X,Y,X) \sim Q(x)W(y|x)Q(x)$.

Fig. 1 compares the error exponents (28), (30) and (24) at SNRs 5 dB and 10 dB. It suggests that $E_{cc}^{(swp,\beta)}(R)$ approaches the constant-composition exponent.

For a more detailed comparison, we introduce error exponent ratios with the iid exponent as the baseline. We call these the relative constant-composition exponent and the relative swapped scaling exponent, respectively given by

$$E_{cc}^{(r)}(R) \triangleq \frac{E_{cc}^{(c)}(R)}{E_{cr}^{(i)}(R)},$$

and

$$E_{cc}^{(swp,\beta)}(R) \triangleq \frac{E_{cc}^{(swp,\beta)}(R)}{E_{cr}^{(i)}(R)}.$$  \hspace{1cm} (32)

Our figures show the relative random-coding exponents as a function of both SNR and the rate $R$ in a single contour plot for coded modulation with a 16QAM constellation and a uniform distribution $Q$. The figures also depict the mutual information (MI) as a solid line and the critical rate $R_{cr}$ of the iid exponent (resp. $R_{cc}^{(c)}$ of the constant-composition exponent) as a dashed (resp. dotted) line.

1) Constant-composition exponent: The constant-composition exponent’s gain with respect to the iid exponent provides a benchmark to assess the performance of the codeword rescaling. The relative exponent is shown in Fig. 2. The figure reveals that the constant-composition exponent exhibits the largest gains for low to moderate SNRs. At high SNRs above 12 dB, it is roughly equal to the iid exponent. A similar tendency is seen at very low SNRs. For our comparison, the most relevant part of the contour plot is located between the critical rates and the MI, since below the critical rate expurgated versions of the exponents lead to better bounds. The maximal gain with respect to the iid exponent is roughly 13 % and occurs around SNR = 5.5 dB and $R = 1.25$ bits per channel use.

2) Swapped exponent with $\beta = 1$: We discuss first the relative swapped exponent with $\beta = 1$, which corresponds to

\[ \text{The critical rate is defined as the largest rate } R \text{ at which the optimal } \rho \text{ in the exponent optimization is one.} \]
the standard decoding rule of maximizing $W^\alpha$. Fig. 3 shows this relative exponent. We observe two regimes in the relevant region between the critical rate and the capacity. Below about 7 dB, there is a gain with respect to the iid exponent, whereas above 7 dB the swapped exponent is worse.

In the low-SNR region and close to the capacity, the swapped exponent achieves similar gains as the constant-composition exponent, namely, about 10% gain at 3 dB and 1.5 bits per channel use. However, it falls short as the rate approaches the critical rate. For example, there is no gain at 5.5 dB and 1.25 bits per channel use, the point where the constant-composition exponent achieves the highest gain. At high SNRs, especially around 14 dB, Fig. 3 unveils a large loss compared to the iid exponent. In this region, we observe not even at capacity a gain and the loss is up to 35% close to the critical rate.

3) Swapped exponent with optimal $\beta$: Optimizing over $\beta$ to adapt the mismatched metric leads to respectable gains in some regions of the SNR-rate plane, as we can see in Fig. 4. At high SNRs, the swapped exponent with optimized $\beta$ exhibits a considerable improvement compared to the swapped exponent with $\beta = 1$, even though it is still below the iid exponent. Most notably, for low SNRs, the swapped exponent with optimized $\beta$ achieves more than 90% of the gain that the constant-composition exponent achieves with respect to the iid exponent. Especially in regions farther away from capacity, the fully optimized exponent shows a large improvement with respect to the one with $\beta = 1$.

REFERENCES