Channel Input Adaptation via Natural Type Selection

Sergey Tridenski and Ram Zamir, *Fellow, IEEE*

***Abstract*— We propose an algorithm for computation of the optimal correct-decoding exponent, and its corresponding optimal input. The computation algorithm translates into a stochastic iterative algorithm for adaptation of the codebook distribution to an unknown discrete memoryless channel in the limit of a large block length. The adaptation scheme uses i.i.d. random block codes, and it relies on one bit of feedback per transmitted block. Throughout the adaptation process, the communication itself is assumed reliable at a constant rate R below the channel capacity C. In the end of the iterations, the resulting codebook distribution guarantees reliable communication for all rates below $R + \Delta$, where $0 < \Delta \leq C - R$ is a predetermined reliability parameter affecting the speed of adaptation.**

***Index Terms*— Correct-decoding exponent, Arimoto algorithm, Blahut algorithm, unknown channels, input distribution.**

I. Introduction

CONSIDER a standard information theoretic scenario of communication through a discrete memoryless channel (DMC), with transition probability $P(y \mid x)$, using block codes. For this case information theory provides optimal solutions in the form of the channel input distribution $Q^*(x)$, achieving the Shannon capacity C or the Gallager error exponent $E(R)$ for a given communication rate R. Suppose, however, that the channel stochastic matrix $P(y \mid x)$ is slowly, or rarely, changing with time and we would like to sustain reliable communication at a constant rate R. For this purpose, we assume the use of a single bit of feedback, from the receiver to the transmitter, per transmitted block (Figure 1). This bit of feedback should tell the transmitter whether to update the codebook or not. In our model, we further assume that the feedback bit and the new codebook are determined using the last pair of the transmitted and received blocks only, i.e. without memory from the previous blocks involved. In this way, potentially, the system will follow the changes in the channel more closely. Our goal of sustaining reliable communication at a constant rate R is legitimate and feasible, of course, only for as long as the capacity of the channel C as a function of $P(y \mid x)$ stays above the rate R. While the channel capacity may stay well above the rate, the optimal solution $Q^*(x)$ may drift significantly, as a result of the drift in $P(y \mid x)$, and render the initial code unreliable.

Manuscript received November 4, 2018; revised August 24, 2019; accepted August 30, 2019. Date of publication September 17, 2019; date of current version March 17, 2020. The work of S. Tridenski and R. Zamir was supported in part by the Israel Science Foundation (ISF), under Grant 676/15 and in part by the US-Israel Binational and US-National Science Foundations (BSF-NSF) under Grant 2018690. This article was presented in part at ISIT2017 [1] and ISIT2018 [13].

The authors are with the Department of Electrical Engineering-Systems, Tel-Aviv University, Tel-Aviv 69978, Israel (e-mail: sergeytr@post.tau.ac.il; zamir@eng.tau.ac.il).

Communicated by N. Merhav, Associate Editor for Shannon Theory.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2941930

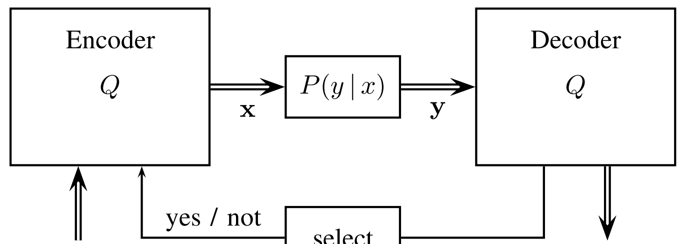

Fig. 1. DMC with a 1-bit feedback per block. Each symbol in the random block code is generated i.i.d. according to $Q(x)$.

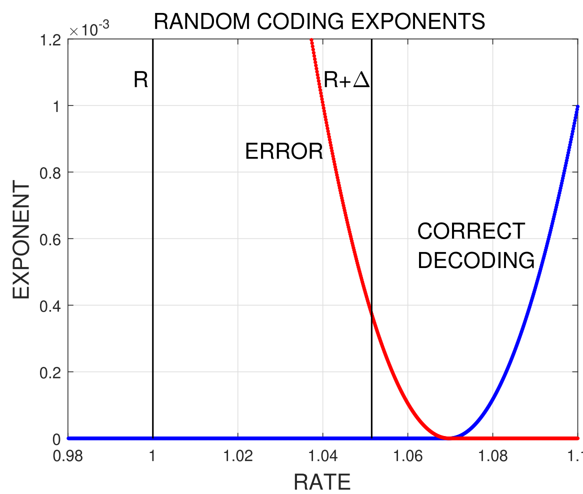

Fig. 2. The i.i.d. random-coding error and correct-decoding exponents for a given Q. Both exponents meet zero at the same point which is the mutual information $I(Q, P)$ associated with the codebook distribution $Q(x)$ and the conditional channel distribution $P(y \mid x)$. The correct-decoding exponent is zero at $R + \Delta$.

In this work the block code is modeled as a random code generated i.i.d. with a distribution Q. The reason for modeling the code as an i.i.d. random code is twofold. Firstly, *random* codes achieve capacity. We consider the maximum-likelihood *correct-decoding* random coding exponent for a given Q [1, eq. 31], [2], as a function of the rate (see Figure 2, which illustrates both the correct-decoding exponent and the error exponent for a given Q). The idea is to choose some positive constant $\Delta > 0$ and to change Q, so that the correct-decoding exponent will be "pinned" to zero at a rate $R' = R + \Delta$, provided that $R + \Delta < C$. This would mean that the corresponding *error* exponent for that Q [3, eq. 5.6.28] is strictly positive for all rates below $R+\Delta$, thus ensuring, in particular, reliable communication at the rate R (Figure 2).

Secondly, an *i.i.d.* distribution in a random code, unlike a distribution over a single type in a constant composition code, results in a certain diversity of codeword types, which allows us to invoke a mechanism of *natural type selection* for update of the parameter Q. Using this mechanism iteratively, we successively update the codebook distribution Q, so that eventually the correct-decoding exponent associated with Q decreases to zero at $R + \Delta$, as desired.

Although our motivation comes from tracking a slowly-varying channel, in our analysis we assume that the channel $P(y \,|\, x)$ remains the same during the iterations.

The mechanism of natural type selection (NTS) has been originally observed and studied in the lossy source-coding setting [4], [5]. In that setting an unknown discrete memoryless source is mapped into a reproduction codebook, generated i.i.d. according to a distribution Q. In the encoding process a linear search is performed through the codebook until the first reproduction sequence is found, which satisfies a distortion constraint D with respect to the source sequence. Since various types are inherently present in the i.i.d. codebook, the empirical distribution of the winning reproduction sequence is in general different from Q and is used for generation of the next codebook. This results in a decrease in the compression rate, which after repeated iterations converges to the optimum given by the rate-distortion function $R(D)$. This last property is guaranteed by the fact that the type of the winning sequence and its conditional type given the source sequence with high probability evolve along the two corresponding steps of the Blahut algorithm for the rate-distortion function computation [6], [7].

We propose an analogous scheme for noisy-channel coding, equipped with its own computation algorithm for channels which is reminiscent of the Blahut algorithm for sources. There is a certain analogy between the distortion constraint D in lossy source-coding and the parameter Δ of the present scheme. The higher is D — the poorer is the reproduction fidelity, but the smaller is the communication penalty $R(D)$. In our case, the higher is Δ — the wider is the gap to capacity $C - R \geq \Delta$, but the higher is the communication reliability $E(R)$.

In a preliminary work [1], we introduced an expression [1, eq. 31] for the correct-decoding exponent for a given Q, which is an alternative to the Dueck-Körner expression in [8]. In particular, the minimization of both expressions over the channel input distribution Q gives the optimal correct-decoding exponent — corresponding to the best sequence of codes for a given rate. The expression for a given Q has the form of a minimum itself, and in the present paper we use it as a vehicle for iterative minimization of the correct-decoding exponent over Q at a fixed rate. The minimization procedure at a fixed rate is comparable to the fixed-*distortion* version of the Blahut algorithm for computation of $R(D)$ [7] and it converges to the optimal exponent and some achieving channel input distribution for the given rate. We translate this iterative minimization procedure at a fixed rate ($R' = R + \Delta$) to a stochastic adaptation scheme, making the assumption that the channel $P(y \,|\, x)$ itself does not change during the iterations.

In [9], we present also a *fixed-slope* version of the same computation. This, in turn, is comparable to the fixed-slope version of the Blahut algorithm for $R(D)$ [6], [10], but also presents an alternative to the Arimoto algorithm for computation of the correct-decoding exponent *function* [2], as well as an alternative to a similar recent algorithm [11].

In Section II we analyze the expression for the correct-decoding exponent presented in [1, eq. 31]. In Section III we introduce our procedure for iterative minimization of the correct-decoding exponent at a fixed rate, and in Section IV we compare it to the fixed-distortion version of the Blahut algorithm [7]. In Section V we present our stochastic adaptation scheme based on the fixed-rate minimization of Section III. Section VI summarizes the paper. Some technical details are deferred to the Appendix.

Notation

The notation $P(y \,|\, x)$ denotes transition probability in a discrete memoryless channel with letters from finite input and output alphabets, $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively. Given a positive real rate R and a blocklength n, a codebook consists of $\lceil e^{nR} \rceil$ codewords of length n, $\mathbf{x}_m \in \mathcal{X}^n$, $m = 1, ..., \lceil e^{nR} \rceil$, generated independently with an i.i.d. distribution Q. The index m represents a message. With a slight abuse of notation, sometimes we also use $Q(x)$ to denote a distribution in the text and in minimization conditions under min, as well as to denote the probability of a symbol x under Q — inside the expressions. We use the same convention for other distributions and empirical distributions as well.

The notation $D(T \circ V \,\|\, T \times Q)$ stands for the Kullback-Leibler divergence from the product distribution $T(y)Q(x)$, denoted as $T \times Q$, to the joint distribution $T(y)V(x \,|\, y)$, denoted as $T \circ V$. By $I(Q, W)$ we mean the mutual information between a pair of random variables with a joint distribution $Q(x)W(y \,|\, x)$.

The notation $|a - b\,|^+$ preserves the difference if $a - b > 0$, and nullifies it otherwise.

By $C(\mathcal{Z})$ we denote the capacity of the channel P if the input is restricted to a subset $\mathcal{Z} \subseteq \mathcal{X}$.

In Section V, where the stochastic scheme is described, we consider empirical distributions (types). In that particular section, if not stated otherwise, $T(y)$ denotes the type of a received block $\mathbf{y} \in \mathcal{Y}^n$, and $V(x \,|\, y)$, or $V_m(x \,|\, y)$, represent the conditional type of a channel input block $\mathbf{x}$, or a codeword $\mathbf{x}_m$, respectively, given the received block $\mathbf{y}$. The type of $\mathbf{x}_m$ is denoted as $T_m(x)$.

II. Correct-Decoding Exponent

The results of this section will allow us to formulate and characterize the computation algorithm in Section III, and the stochastic adaptation scheme in Section V.

A. Implicit Expressions

We will use the following expression for the correct-decoding exponent for a given codebook distribution Q and a communication rate R [1, eq. 32]:

$$E_c^{ML}(R, Q) \triangleq \min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \,\|\, Q \circ P) + \big|R - D(T \circ V \,\|\, T \times Q)\big|^{+} \Big\}, \tag{1}$$

where the minimization is over the joint distribution $T(y)V(x\,|\,y)$, with $y \in \mathcal{Y}$ and $x \in \mathcal{X}$. It can be shown [1, eq. 32], [9], that the expression (1) has the meaning of the maximum-likelihood (ML) correct-decoding exponent of a random code ensemble of rate R generated i.i.d. with a distribution Q. This expression can be easily compared to and shown to be lower (better) than the corresponding constant-composition correct-decoding exponent for a given Q:

$$\begin{aligned} E_c^{ML}(R, Q) &= \min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \,\|\, Q \circ P) + \big|R - \underbrace{D(T \circ V \,\|\, T \times Q)}_{= I(U,W) + D(U \,\|\, Q)}\big|^{+} \Big\} \\ &\equiv \min_{U(x),\, W(y\,|\,x)} \Big\{ D(U \circ W \,\|\, Q \circ P) + \big|R - I(U, W) - D(U \,\|\, Q)\big|^{+} \Big\} \\ &\overset{U=Q}{\leq} \min_{W(y\,|\,x)} \Big\{ D(Q \circ W \,\|\, Q \circ P) + \big|R - I(Q, W)\big|^{+} \Big\}. \end{aligned} \tag{2}$$

After minimization over the codebook distribution Q, the expression (2) can be recognized as the correct-decoding exponent of Dueck and Körner [8], which is optimal. Since the optimal expression cannot be decreased, the minimum of the achievable lower bound (1) over Q is also optimal.

As a stepping stone towards our adaptation scheme, we will use also a closely related expression, which is in general an upper bound on (1) and coincides with it for low R:

$$E_c(R, Q) \triangleq \min_{\substack{T(y),\, V(x\,|\,y):\\ D(T \circ V \,\|\, T \times Q) \geq R}} \Big\{ D(T \circ V \,\|\, Q \circ P) \Big\}. \tag{3}$$

The expression (3) can also be compared to its constant-composition counterpart:

$$\begin{aligned} E_c(R, Q) &= \min_{\substack{T(y),\, V(x\,|\,y):\\ D(T \circ V \,\|\, T \times Q) \geq R}} \Big\{ D(T \circ V \,\|\, Q \circ P) \Big\} \\ &\leq \min_{\substack{U(x),\, W(y\,|\,x):\\ I(U, W) \geq R}} \Big\{ D(U \circ W \,\|\, Q \circ P) \Big\} \\ &\overset{U=Q}{\leq} \min_{\substack{W(y\,|\,x):\\ I(Q, W) \geq R}} \Big\{ D(Q \circ W \,\|\, Q \circ P) \Big\}. \end{aligned} \tag{4}$$

As we shall see, the minimum of (3) over Q, just like the minimum of (1) and (2) over Q, also achieves the optimum for all R. This is not the case with its constant-composition upper bound (4). For sufficiently large R the minimum (4) inevitably becomes $+\infty$, because the mutual information $I(Q, W)$ is upper-bounded by the entropy of Q.

The computation algorithm described in Section III computes iteratively the minimum of (1) or (3) over Q for a given R.

Both minima (1) and (3) represent monotonic functions of R. In what follows, we characterize the minimizing distributions of (1) and (3) with the help of supporting lines (of slopes $-\rho \geq 0$) to the graphs of these functions. Using the supporting lines of slopes $0 \leq -\rho \leq 1$, we also solve the minima (1) and (3) where possible, and express them and their minimizing distributions *explicitly* with the system ingredients R, $Q(x)$, $P(y\,|\,x)$, and the slope parameter ρ. Both the characterization with the supporting lines and the explicit solutions will be used in the analysis of the computation algorithm in the later sections. The minimizing distributions will represent (asymptotically) the selected types in our stochastic adaptation scheme of Section V.

B. Explicit Expressions

The next two lemmas (Lemmas 1 and 2) relate the graphs of the two functions of R, (3) and (1), respectively, to their lower supporting lines of slopes $-\rho \geq 0$, and with their help characterize the minimizing distributions of (3) and (1) at the points where these supporting lines touch the graphs. The expressions for the supporting lines then allow an explicit solution (Lemma 3). The lower supporting lines form a lower convex envelope for each of the two graphs of (3) and (1). Afterwards we examine the relationship between the graphs of (3) and (1) and their lower convex envelopes and state the results in a final lemma (Lemma 4). Lemma 4 will replace, where possible, the minima (3) and (1) with a "Gallager type" expression — a maximization of $E_0(\rho, Q) - \rho R$ over a slope parameter ρ, and will describe the minimizing solutions.

Lemma 1 (Supporting lines for $E_c(R, Q)$): For any $\rho \leq 0$, the minimum (3) is lower-bounded as

$$E_c(R, Q) \geq \min_{\substack{T(y),\, V(x\,|\,y):\\ \mathrm{supp}(V) \subseteq \mathrm{supp}(Q)}} \Big\{ D(T \circ V \,\|\, Q \circ P) - \rho\big[R - D(T \circ V \,\|\, T \times Q)\big] \Big\}. \tag{5}$$

In case of equality in (5), any minimizing solution $T_R \circ V_R$ of the LHS is also a minimizing solution $T_\rho \circ V_\rho$ of the RHS such that $R = D\big(T_\rho \circ V_\rho \,\|\, T_\rho \times Q\big)$, or $R \leq D\big(T_0 \circ V_0 \,\|\, T_0 \times Q\big)$ for $\rho = 0$. Conversely, if there exists a solution $T_\rho \circ V_\rho$ minimizing the RHS, such that $R = D\big(T_\rho \circ V_\rho \,\|\, T_\rho \times Q\big)$, or $R \leq D\big(T_0 \circ V_0 \,\|\, T_0 \times Q\big)$ for $\rho = 0$, then it is also a minimizing solution of the LHS and there is equality in (5).

Proof: The proof is given in Appendix A. □

Lemma 2 (Supporting lines for $E_c^{ML}(R,Q)$): For any $\rho \in [-1,0]$, the minimum (1) is lower-bounded as

$$E_c^{ML}(R,Q) \geq \min_{\substack{T(y),\, V(x\,|\,y):\\ \mathrm{supp}(V)\subseteq\mathrm{supp}(Q)}} \Big\{D(T\circ V\,\|\,Q\circ P) - \rho\big[R - D(T\circ V\,\|\,T\times Q)\big]\Big\}. \quad (6)$$

In case of equality in (6), any minimizing solution $T_R \circ V_R$ of the LHS is also a minimizing solution $T_\rho \circ V_\rho$ of the RHS such that $R = D\big(T_\rho\circ V_\rho\,\|\,T_\rho\times Q\big)$, or $R \leq D\big(T_0\circ V_0\,\|\,T_0\times Q\big)$ for $\rho = 0$, or $R \geq D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big)$ for $\rho = -1$. Conversely, if there exists such a solution $T_\rho\circ V_\rho$ minimizing the RHS, then it is also a minimizing solution of the LHS and there is equality in (6).

Proof: The proof is given in Appendix B. □

Explicit solution of the RHS of (6) gives

Lemma 3 (Explicit solution): For[1] $\rho \geq -1$

$$\min_{\substack{T(y),\, V(x\,|\,y):\\ \mathrm{supp}(V)\subseteq\mathrm{supp}(Q)}} \Big\{D(T\circ V\,\|\,Q\circ P) + \rho D(T\circ V\,\|\,T\times Q)\Big\} = E_0(\rho,Q), \quad (7)$$

where[2]

$$E_0(\rho,Q) \triangleq -\log\sum_y\left[\sum_x Q(x)P^{\frac{1}{1+\rho}}(y\,|\,x)\right]^{1+\rho}, \ \rho > -1, \quad (8)$$

$$E_0(-1,Q) \triangleq \lim_{\rho\searrow -1} E_0(\rho,Q) = -\log\sum_y \max_{\substack{x:\\ Q(x)>0}} P(y\,|\,x). \quad (9)$$

If $\rho > -1$, then the unique minimizing solution of (7) is given by $T_\rho \circ V_\rho$ with

$$T_\rho(y) \propto \left[\sum_a Q(a)P^{\frac{1}{1+\rho}}(y\,|\,a)\right]^{1+\rho}, \quad (10)$$

$$V_\rho(x\,|\,y) \propto Q(x)P^{\frac{1}{1+\rho}}(y\,|\,x). \quad (11)$$

If $\rho = -1$, then all minimizing solutions of (7) are given by any $T_{-1}\circ V_{-1}$ such that

$$T_{-1}(y) \propto \max_{a:\,Q(a)>0} P(y\,|\,a), \quad (12)$$

$$V_{-1}(x\,|\,y) = 0, \quad \forall\, x \notin \arg\max_{a:\,Q(a)>0} P(y\,|\,a). \quad (13)$$

Proof: The proof is given in Appendix C. □

Since the minimizing distribution $V_{-1}(x\,|\,y)$ of (7) with $\rho = -1$ is allowed to be arbitrary inside its support which is restricted according to (13), for convenience let us define

$$R_{-1}^{-}(Q) \triangleq \min_{V_{-1}(x\,|\,y)} D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big), \quad (14)$$

$$R_{-1}^{+}(Q) \triangleq \max_{V_{-1}(x\,|\,y)} D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big), \quad (15)$$

where the min and max are over all $V_{-1}(x\,|\,y)$ as in (13).

[1]A solution can be obtained also for $\rho < -1$ by maximization of a convex (∪) function.

[2]For $-1 < \rho \leq 0$ the Arimoto algorithm [2] computes $\min_Q E_0(\rho,Q)$.

The supporting lines, described by Lemmas 1 and 2, form the lower convex envelopes for the graphs of (3) and (1), respectively. Next, using Lemma 3, we partially determine — where these lower convex envelopes coincide with the respective graphs of (3) and (1), and characterize the minimizing distributions there. The partial result will be sufficient for the analysis in the next section.

Lemma 4 (Explicit formula and minimizing solutions):

$$E_c(R,Q) = \max_{-1\leq\rho\leq 0}\big\{E_0(\rho,Q) - \rho R\big\}, \quad \forall\, R \leq R_{-1}^{+}(Q), \quad (16)$$

$$E_c^{ML}(R,Q) \equiv \max_{-1\leq\rho\leq 0}\big\{E_0(\rho,Q) - \rho R\big\}, \quad (17)$$

where $E_0(\rho,Q)$ is defined by (8)-(9), $R_{-1}^{+}(Q)$ defined in (15), and $T_{-1}\circ V_{-1}$ is a family of distributions defined by (12)-(13). If the RHS of (17) is maximized by $\rho = -1$, then all minimizing solutions of the LHS are given by $T_{-1}\circ V_{-1}$ as in (12)-(13) such that $D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big) \leq R$. If the RHS of (16) is maximized by $\rho = -1$, then all minimizing solutions of the LHS are given by $T_{-1}\circ V_{-1}$ as in (12)-(13) such that $D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big) = R$. If the RHS of (17) is maximized by $\rho \in (-1,0]$, then the unique minimizing solution of the LHS is given by (10)-(11). Same for (16).

Proof: For $\rho \in (-1,0]$ and $R = D\big(T_\rho\circ V_\rho\,\|\,T_\rho\times Q\big)$, Lemmas 1, 2 give equalities in (5), (6), respectively, with the same unique distribution $T_\rho\circ V_\rho$ given by (10)-(11) of Lemma 3, minimizing both sides of each equality. Observe that two different slope parameters $-1 \leq \alpha < \beta \leq 0$ of two lower supporting lines from Lemma 1 or 2 satisfy necessarily $D\big(T_\beta\circ V_\beta\,\|\,T_\beta\times Q\big) \leq D\big(T_\alpha\circ V_\alpha\,\|\,T_\alpha\times Q\big)$. Since $D\big(T_\rho\circ V_\rho\,\|\,T_\rho\times Q\big) \equiv \frac{\partial E_0(\rho,Q)}{\partial\rho}$ is a continuous function of $\rho > -1$, this covers all R such that

$$D\big(T_0\circ V_0\,\|\,T_0\times Q\big) \leq R \leq \lim_{\rho\searrow -1} D\big(T_\rho\circ V_\rho\,\|\,T_\rho\times Q\big).$$

For $\rho = 0$ and $R \leq D\big(T_0\circ V_0\,\|\,T_0\times Q\big) \equiv \frac{\partial E_0(\rho,Q)}{\partial\rho}\Big|_{\rho=0}$, Lemmas 1, 2 give equalities in (5), (6), respectively, with the unique minimizing distribution $T_0\circ V_0 \equiv Q\circ P$ on both sides.

The minimum $R_{-1}^{-}(Q)$ defined in (14) is achieved by

$$V_{-1}(x\,|\,y) \propto \begin{cases} Q(x), & x \in \arg\max_{a:\,Q(a)>0} P(y\,|\,a),\\ 0, & \text{else.}\end{cases}$$

This allows for continuity $\lim_{\rho\searrow -1} D\big(T_\rho\circ V_\rho\,\|\,T_\rho\times Q\big) = R_{-1}^{-}(Q)$.

For $\rho = -1$ and $R \geq R_{-1}^{-}(Q)$, Lemma 2 gives equality in (6) with all possible solutions of the minimum on the LHS of (6) as given by Lemma 3 in (12)-(13) and such that $R \geq D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big)$. Lemma 1 gives equality in (5) with all possible solutions of the minimum on the LHS of (5) as given by Lemma 3 in (12)-(13) and such that $D\big(T_{-1}\circ V_{-1}\,\|\,T_{-1}\times Q\big) = R$. □

In the next sections we will use Lemmas 2, 3, and 4.

It follows from Lemma 4 that the minima (1) and (3) coincide for $R \leq R_{-1}^{+}(Q)$. For greater R the ML exponent

(1) continues to grow with the increase of R with the constant slope $-\rho = 1$, according to (17). The graph of the function (3), on the other hand, by Lemma 1 has supporting lines also with slopes greater than 1. Therefore (3) may become higher than (17), and eventually it always exhibits a jump to infinity at some $R \geq R_{-1}^{+}(Q)$.

Both (3) and (1) have a supporting line $E_0(-1, Q) + R = E(R)$ of slope 1. This supporting line is invariant in the sense that it depends only on the support of the distribution $Q(x)$ according to the expression for $E_0(-1, Q)$ in (9). Since the rate $R = D\big(T_{-1} \circ V_{-1} \parallel T_{-1} \times Q\big)$, where both functions meet this supporting line, can be made arbitrarily large by reducing $Q(x)$ on some letter x, the minimum over Q of (3) can always achieve the minimum over Q of (1) for any R:

$$\min_{Q} E_c(R, Q) = \min_{Q} E_c^{ML}(R, Q) \triangleq E_c(R), \quad \forall R. \tag{18}$$

Therefore both expressions (3) and (1) achieve the optimum. For comparison, this is not possible with the constant-composition expression (4) where the mutual information is bounded by the entropy in the support of Q.

III. Iterative Minimization of the Correct-Decoding Exponent

Here we propose a procedure of iterative minimization with (1) or (3) at fixed rate R, which leads to the optimal correct-decoding exponent (18). This can be termed also as a fixed-rate computation of the correct-decoding exponent and is different than the algorithm of Arimoto [2] for computation of the exponent function $\min_Q E_0(\rho, Q)$. The difference is both in the fact that the Arimoto algorithm is a computation at a fixed slope ρ, but also the computation itself is different. The advantage of the fixed-rate computation over the fixed-slope is that we know how to translate it to a stochastic adaptation procedure.

The next lemma presents and characterizes the iterative minimization procedure for the ML exponent (1).

Lemma 5 (Monotonicity for $E_c^{ML}(R, Q)$): An iterative update of the parameter Q in (1) by its minimizing solution $\check{T}(y)\check{V}(x \mid y)$:

$$\check{T}_\ell(y)\check{V}_\ell(x \mid y) \in \arg \min_{T(y),\, V(x \mid y)} \Big\{ D(T \circ V \parallel Q_\ell \circ P) + \big|R - D(T \circ V \parallel T \times Q_\ell)\big|^{+} \Big\}, \tag{19}$$

$$Q_{\ell+1}(x) \leftarrow \sum_y \check{T}_\ell(y)\check{V}_\ell(x \mid y) \tag{20}$$

results in a monotonically non-increasing sequence $\big\{E_c^{ML}(R, Q_\ell)\big\}_{\ell=0}^{+\infty}$ of (1). At each step, the sequence decreases at least by an amount $(1 + \hat{\rho}_{\ell+1}) D(Q_{\ell+1} \parallel Q_\ell)$, where $\hat{\rho}_{\ell+1} \in [-1, 0]$ is a parameter of some supporting line (6) touching the graph of $E_c^{ML}(R, Q_{\ell+1})$ at R.

Proof: By Lemma 4 / Lemma 3, the graph of $E_c^{ML}(R, Q)$ touches at R some supporting line of the form (6) with some slope parameter $\hat{\rho} \in [-1, 0]$. A solution $\check{T} \circ \check{V}$ of (1) according to Lemma 2 is also a solution of (6) with $\hat{\rho}$ and we can write:

$$\begin{aligned}
&E_c^{ML}(R, Q) \\
&\overset{\text{touch}}{=} D(\check{T} \circ \check{V} \parallel Q \circ P) - \hat{\rho}\big[R - D(\check{T} \circ \check{V} \parallel \check{T} \times Q)\big] \\
&\overset{(a)}{=} \max_{-1 \leq \rho \leq 0} \Big\{ D(\check{T} \circ \check{V} \parallel Q \circ P) - \rho\big[R - D(\check{T} \circ \check{V} \parallel \check{T} \times Q)\big] \Big\} \\
&\overset{(b)}{\geq} \max_{-1 \leq \rho \leq 0} \Big\{ D(\check{T} \circ \check{V} \parallel \check{Q} \circ P) - \rho\big[R - D(\check{T} \circ \check{V} \parallel \check{T} \times \check{Q})\big] \Big\} \\
&\geq \max_{-1 \leq \rho \leq 0} \min_{\substack{T(y),\, V(x \mid y): \\ \text{supp}(V) \subseteq \text{supp}(\check{Q})}} \Big\{ D(T \circ V \parallel \check{Q} \circ P) - \rho\big[R - D(T \circ V \parallel T \times \check{Q})\big] \Big\} \\
&\overset{(c)}{=} E_c^{ML}(R, \check{Q}),
\end{aligned}$$

where $\check{Q}(x) = \sum_y \check{T}(y)\check{V}(x \mid y)$, and

(a) holds because for $\hat{\rho} \in (-1, 0)$ Lemma 2 gives $R = D(\check{T} \circ \check{V} \parallel \check{T} \times Q)$ and the brackets are zero. For $\hat{\rho} = 0$ Lemma 2 gives $R \leq D(\check{T} \circ \check{V} \parallel \check{T} \times Q)$, so that the brackets are non-positive and the maximum is at $\rho = 0$. In the case $\hat{\rho} = -1$, Lemma 2 gives $R \geq D(\check{T} \circ \check{V} \parallel \check{T} \times Q)$, so that the brackets are non-negative and the maximum is at $\rho = -1$.

(b) holds because by replacing $Q(x)$ with $\check{Q}(x) = \sum_y \check{T}(y)\check{V}(x \mid y)$ we obtain in the expression

$$\begin{aligned}
&D(\check{T} \circ \check{V} \parallel Q \circ P) + \rho D(\check{T} \circ \check{V} \parallel \check{T} \times Q) \\
&= D(\check{T} \circ \check{V} \parallel \check{Q} \circ P) + \rho D(\check{T} \circ \check{V} \parallel \check{T} \times \check{Q}) \\
&\quad + \underbrace{(1 + \rho) D(\check{Q} \parallel Q)}_{\geq 0} \qquad (21) \\
&\geq D(\check{T} \circ \check{V} \parallel \check{Q} \circ P) + \rho D(\check{T} \circ \check{V} \parallel \check{T} \times \check{Q}).
\end{aligned}$$

(c) holds by (17) and (7).

The monotonicity of the sequence of $E_c^{ML}(R, Q_\ell)$ follows by viewing Q as Q_ℓ and $\check{Q}(x)$ as $Q_{\ell+1}$, and the bound on the amount of decrease follows from (21). □

Note that, whenever $\hat{\rho}_\ell \in (-1, 0]$, the computation in (19) goes along (10)-(11) with $\hat{\rho}_\ell$, which results in a ratio $Q_{\ell+1}(x)/Q_\ell(x)$ different than in the Arimoto computation of $Q_{\ell+1}$ from Q_ℓ [2, eq. 24-25] for the same $\hat{\rho}_\ell$. Besides, the slope parameter $\hat{\rho}_\ell$ itself is changing here in each iteration.

The monotonicity of the sequence of $E_c^{ML}(R, Q_\ell)$ implies convergence, but not necessarily all the way down to the optimal exponent (18), and in principle the limit may stay above it. The following theorem tries to characterize the convergence of the above minimization procedure.

Theorem 1 (Convergence of iterations for $E_c^{ML}(R, Q)$): Let $\Big\{\big(\check{T}_\ell, \check{V}_\ell\big)\Big\}_{\ell=0}^{+\infty}$ be a sequence of iterative solutions of (1) with $Q = Q_\ell$ obtained by (20). Then

$$E_c^{ML}(R, Q_\ell) \overset{\ell \to \infty}{\searrow} \min_{Q:\ \text{supp}(Q) \subseteq \mathcal{Z}} E_c^{ML}(R, Q), \tag{22}$$

for some $\mathcal{Z} \subseteq \text{supp}(Q_0)$.

Proof: By Lemma 4 / Lemma 3, the graph of $E_c^{ML}(\widetilde{R}, Q_\ell)$ touches at $\widetilde{R} = R$ some supporting line of the form (6), not necessarily unique. Let us choose a slope parameter of one such line $\hat{\rho}_\ell \in [-1, 0]$ for each index ℓ. Then we have a sequence of pairs $\Big\{\big(Q_\ell, \hat{\rho}_\ell\big)\Big\}_{\ell=0}^{+\infty}$. By Lemma 4, the distribution Q_ℓ is updated for the next time $\ell+1$ according to either (10)-(11) with $\hat\rho_\ell \in (-1,0]$ or (12)-(13) if $\hat\rho_\ell = -1$. In both cases the support of the distribution Q_ℓ cannot increase. It can decrease by (13), or the distribution Q_ℓ can approach arbitrarily close to zero for some letters of the channel input alphabet where the initial value of Q_0 is positive. Consider a convergent subsequence of adjacent pairs $\big\{\big(Q_{\ell_i},\, \hat\rho_{\ell_i},\, Q_{\ell_i+1},\, \hat\rho_{\ell_i+1}\big)\big\}_{i=1}^{+\infty}$:

$$Q_{\ell_i} \underset{i\to\infty}{\longrightarrow} \overline{Q}_1, \qquad \hat\rho_{\ell_i} \underset{i\to\infty}{\longrightarrow} \bar\rho_1 \in [-1,0],$$
$$Q_{\ell_i+1} \underset{i\to\infty}{\longrightarrow} \overline{Q}_2, \qquad \hat\rho_{\ell_i+1} \underset{i\to\infty}{\longrightarrow} \bar\rho_2 \in [-1,0].$$

We have $\operatorname{supp}(\overline{Q}_j) \subseteq \operatorname{supp}(Q_0)$, $j=1,2$.

Let us first examine the limit of the graph of $E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big)$ as a function of $\widetilde{R}$. For any $\beta \in (0,1)$ arbitrarily close to 1 and a large enough index i we can write according to (17) and (9):

$$\sup_{-1<\rho\le 0}\left\{-\log\sum_y\left[\sum_x \underbrace{\beta\overline{Q}_1(x)}_{\le Q_{\ell_i}(x)} P^{\frac{1}{1+\rho}}(y\,|\,x)\right]^{1+\rho} - \rho\widetilde{R}\right\}$$
$$\ge\; E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big) \;\ge\; \max_{-\beta\le\rho\le 0}\Big\{E_0\big(\rho,\, Q_{\ell_i}\big) - \rho\widetilde{R}\Big\}.$$

Now it is convenient to take i to $+\infty$ in the lower bound. From which we obtain for any $\beta\in(0,1)$:

$$\max_{-1\le\rho\le 0}\Big\{E_0(\rho,\overline{Q}_1) - (1+\rho)\log\beta - \rho\widetilde{R}\Big\} \;\ge$$
$$\limsup_{i\to\infty} E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big) \;\ge\; \liminf_{i\to\infty} E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big) \;\ge$$
$$\max_{-\beta\le\rho\le 0}\Big\{E_0(\rho,\overline{Q}_1) - \rho\widetilde{R}\Big\}.$$

Then by continuity of $E_0(\rho,\overline{Q}_1)$, as a function of ρ, (9), and (17), we obtain

$$\lim_{i\to\infty} E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big) \;=\; E_c^{ML}(\widetilde{R},\overline{Q}_1), \qquad \forall\,\widetilde{R}.$$

In particular, the supporting lines $E_0\big(\hat\rho_{\ell_i},\, Q_{\ell_i}\big) - \hat\rho_{\ell_i}\widetilde{R}$ of $E_c^{ML}\big(\widetilde{R},\, Q_{\ell_i}\big)$ converge to the supporting line of $E_c^{ML}(\widetilde{R},\overline{Q}_1)$ with slope parameter $\bar\rho_1$, which is given by $E_0(\bar\rho_1,\overline{Q}_1) - \bar\rho_1\widetilde{R}$. At $\widetilde{R}=R$ this gives $E_c^{ML}\big(R,\, Q_{\ell_i}\big) \to E_0(\bar\rho_1,\overline{Q}_1) - \bar\rho_1 R$. Similarly we obtain $E_c^{ML}\big(R,\, Q_{\ell_i+1}\big) \to E_0(\bar\rho_2,\overline{Q}_2) - \bar\rho_2 R$.

If $\bar\rho_1 = 0$ or $\bar\rho_2 = 0$, then $E_c^{ML}\big(R,\, Q_{\ell_i}\big) \searrow 0$ by the above result and monotonicity of Lemma 5.

If $\bar\rho_1 = -1$, then $E_c^{ML}\big(R,\, Q_{\ell_i}\big) \searrow E_0(-1,\overline{Q}_1) + R$. By (17) and (9), we conclude that this is the minimum of $E_c^{ML}(R,Q)$ over all Q with $\operatorname{supp}(Q)\subseteq\operatorname{supp}(\overline{Q}_1)$. Similarly, if $\bar\rho_2 = -1$, then $E_c^{ML}\big(R,\, Q_{\ell_i}\big) \searrow E_0(-1,\overline{Q}_2) + R$, which is the minimum of $E_c^{ML}(R,Q)$ over all Q with $\operatorname{supp}(Q)\subseteq\operatorname{supp}(\overline{Q}_2)$.

Suppose now that $\bar\rho_1, \bar\rho_2 \in (-1,0)$. Since $\bar\rho_1 \in (-1,0)$, then also $\hat\rho_{\ell_i} \in (-1,0)$ for a large enough index i, and the distribution Q_{ℓ_i} is updated for the next time ℓ_i+1 according to (10)-(11) as:

$$Q_{\ell_i+1}(x) \;=$$
$$\frac{1}{K_i}\,Q_{\ell_i}(x)\sum_{y:\,P(y\,|\,x)>0} P^{\gamma_i}(y\,|\,x)\left[\sum_a Q_{\ell_i}(a)P^{\gamma_i}(y\,|\,a)\right]^{\hat\rho_{\ell_i}},$$
$$\gamma_i \;\triangleq\; (1+\hat\rho_{\ell_i})^{-1}. \tag{23}$$

In the limit where $\overline{Q}_1(x)$ is positive, (23) becomes

$$\overline{Q}_2(x) \;=$$
$$\frac{1}{K}\,\overline{Q}_1(x)\sum_{y:\,P(y\,|\,x)>0} P^{\gamma}(y\,|\,x)\left[\sum_a \overline{Q}_1(a)P^{\gamma}(y\,|\,a)\right]^{\bar\rho_1},$$
$$\gamma \;\triangleq\; (1+\bar\rho_1)^{-1}. \tag{24}$$

Since also $\bar\rho_2 \in (-1,0)$, then $1+\hat\rho_{\ell_i+1}$ converges to a positive number and by Lemma 5 necessarily $D\big(Q_{\ell_i+1}\,\|\,Q_{\ell_i}\big) \to 0$. In this case also $Q_{\ell_i+1} \to \overline{Q}_1$, i.e. necessarily $\overline{Q}_1 = \overline{Q}_2$. Dividing both sides of (24) by $\overline{Q}_1(x)$ where it is positive, for all such x we obtain:

$$\sum_{y:\,P(y\,|\,x)>0} P^{\gamma}(y\,|\,x)\left[\sum_a \overline{Q}_1(a)P^{\gamma}(y\,|\,a)\right]^{\bar\rho_1} \;=\; K,$$
$$\overline{Q}_1(x) > 0. \tag{25}$$

This can be recognized as a sufficient condition for $\overline{Q}_1$ to minimize $E_0(\bar\rho_1, Q)$ over all Q with $\operatorname{supp}(Q)\subseteq\operatorname{supp}(\overline{Q}_1)$, the same as [2, eq. 22]. By (17), we conclude that the limit of $E_c^{ML}\big(R,\, Q_{\ell_i}\big)$, which is given by $E_0(\bar\rho_1,\overline{Q}_1) - \bar\rho_1 R$, is the minimum of $E_c^{ML}(R,Q)$ over such Q. □

Let $C(\mathcal{Z})$ denote the capacity of the channel with an input alphabet $\mathcal{Z}\subseteq\mathcal{X}$. Observe that for any $R>0$ holds

$$\min_{\mathcal{Z}:\;C(\mathcal{Z})<R}\;\min_{Q:\;\operatorname{supp}(Q)\subseteq\mathcal{Z}} E_c^{ML}(R,Q) \;=\; \min_{Q:\;C(\operatorname{supp}(Q))<R} E_c^{ML}(R,Q) \;>\; 0.$$

This observation conveniently allows us to grasp and write one sufficient condition for the convergence of the iterative minimization using (1) described by Lemma 5, and also of the analogous procedure for (3), all the way to the minimum over Q (18), when this minimum is zero.

Lemma 6 (Convergence to zero for $E_c^{ML}(R,Q)$): Let $\big\{\big(\check{T}_\ell,\check{V}_\ell\big)\big\}_{\ell=0}^{+\infty}$ be a sequence of iterative solutions of (1) with $Q=Q_\ell$ obtained by (20).

If the initial distribution Q_0 satisfies the strict inequality:

$$E_c^{ML}(R,Q_0) \;<\; \min_{Q:\;C(\operatorname{supp}(Q))<R} E_c^{ML}(R,Q), \tag{26}$$

then

$$E_c^{ML}(R,Q_\ell) \;\overset{\ell\to\infty}{\searrow}\; 0.$$

Proof: By Theorem 1, the resultant sequence of $E_c^{ML}(R,Q_\ell)$ must monotonically converge to a minimum of $E_c^{ML}(R,Q)$ over Q with $\operatorname{supp}(Q)\subseteq\mathcal{Z}$ for some subset of the channel input alphabet $\mathcal{Z}\subseteq\mathcal{X}$. Suppose that $C(\mathcal{Z}) < R$. Then also for every subset $\operatorname{supp}(Q)\subseteq\mathcal{Z}$ we have $C\big(\operatorname{supp}(Q)\big) < R$. Then the limit of the sequence of

$E_c^{ML}(R, Q_\ell)$ must be lower-bounded by the minimum on the RHS of (26). This is a contradiction, since the monotonically non-increasing sequence must be upper-bounded by its first element $E_c^{ML}(R, Q_0)$ on the LHS of the strict inequality (26). We conclude that necessarily $C(\mathcal{Z}) \geq R$. In particular, there exists some Q with $\text{supp}(Q) \subseteq \mathcal{Z}$ such that $I(Q, P) \geq R$. This gives $E_c^{ML}(R, Q) = 0$ by (1) for this Q. Consequently the minimum in (22) is zero. □

Note that for each $0 < R \leq C(\mathcal{X})$ — there exist such initial input distributions Q_0 that satisfy the condition (26) of Lemma 6. Therefore (26) guarantees a region of convergence of (1) to the optimal exponent (18) as a result of the iterative procedure (19)-(20) for $0 < R \leq C(\mathcal{X})$. Next, we extend the above result from (1) to (3).

Lemma 7: $E_0(-1, Q) + C\big(\text{supp}(Q)\big) \leq 0$.

Proof: Suppose on the contrary that $E_0(-1, Q) + C\big(\text{supp}(Q)\big) > 0$. Then

$$\min_{\widetilde{Q}:\ \text{supp}(\widetilde{Q}) \subseteq \text{supp}(Q)} E_c^{ML}\big(C\big(\text{supp}(Q)\big),\ \widetilde{Q}\big) \overset{(17)}{\geq} \min_{\widetilde{Q}:\ \text{supp}(\widetilde{Q}) \subseteq \text{supp}(Q)} \Big\{E_0(-1, \widetilde{Q}) + C\big(\text{supp}(Q)\big)\Big\} \overset{(9)}{\geq} \min_{\widetilde{Q}:\ \text{supp}(\widetilde{Q}) \subseteq \text{supp}(Q)} \Big\{E_0(-1, Q) + C\big(\text{supp}(Q)\big)\Big\} > 0.$$

The minimal correct-decoding exponent $\min_{\widetilde{Q}} E_c^{ML}\big(R, \widetilde{Q}\big)$ of the channel with the input alphabet $\text{supp}(Q)$ appears to be positive at $R = C\big(\text{supp}(Q)\big)$, which is a contradiction. □

Lemma 8: $C\big(\text{supp}(Q)\big) \leq R_{-1}^{-}(Q)$*, as defined in (14).*

Proof: According to Lemma 7, $E_0(-1, Q) + C\big(\text{supp}(Q)\big) \leq 0$. This means that, by Lemmas 2, 3, and definition (14), the supporting line $E(\widetilde{R}) = E_0(-1, Q) + \widetilde{R}$ of slope 1 touches the graph of $E_c^{ML}(\widetilde{R}, Q)$ at $\widetilde{R} = R_{-1}^{-}(Q) \geq C\big(\text{supp}(Q)\big)$. □

Lemma 9 (One iteration):
If $C\big(\text{supp}(Q)\big) \geq R$ *then the following holds:*
a) $E_c(R, Q) = E_c^{ML}(R, Q)$*, as defined in (3) and (1), sharing the same solution* $(\check{T}, \check{V})$*,*
b) $\check{Q}(x) = \sum_y \check{T}(y)\check{V}(x \mid y)$ *satisfies* $\text{supp}(\check{Q}) = \text{supp}(Q)$*.*

Proof: Lemma 8 together with Lemma 4 imply that two things hold ((i) and (ii)):
i) the graphs of $E_c^{ML}(\widetilde{R}, Q)$ and $E_c(\widetilde{R}, Q)$ coincide for all $\widetilde{R} \leq C\big(\text{supp}(Q)\big)$ and
ii) the corresponding minima (1) and (3) share the same minimizing solutions there.
In particular, this holds at $\widetilde{R} = R \leq C\big(\text{supp}(Q)\big)$. Then $E_c^{ML}(R, Q) = E_c(R, Q)$, sharing the same solutions $(\check{T}, \check{V})$. Since $C\big(\text{supp}(Q)\big) \geq R$, Lemmas 7 and 4 imply also that the graph of $E_c^{ML}(\widetilde{R}, Q)$ touches at $\widetilde{R} = R$ some supporting line with slope parameter $\rho \in (-1, 0]$. Then, by Lemma 4, the unique solution $(\check{T}, \check{V})$ is determined according to (10)-(11). Then $\text{supp}(\check{Q}) = \text{supp}(Q)$. □

Lemma 10 (Convergence of iterations for $E_c(R, Q)$ *):*
Let $\Big\{\big(\check{T}_\ell, \check{V}_\ell\big)\Big\}_{\ell=0}^{+\infty}$ *be a sequence of iterative solutions of (3) with* $Q = Q_\ell$ *at each iteration obtained from the previous solution as in (20). If the initial distribution satisfies* $C\big(\text{supp}(Q_0)\big) \geq R$*, then for each* ℓ *holds* $E_c(R, Q_\ell) = E_c^{ML}(R, Q_\ell)$*, (1), sharing the same solution* $\big(\check{T}_\ell, \check{V}_\ell\big)$*.*

Proof: Follows from Lemma 9 by induction. □

Now we can state the parallel of Lemma 6 for the upper bound (3) on the ML correct-decoding exponent.

Theorem 2 (Convergence to zero for $E_c(R, Q)$ *):*
Let $\Big\{\big(\check{T}_\ell, \check{V}_\ell\big)\Big\}_{\ell=0}^{+\infty}$ *be a sequence of iterative solutions of (3) with* $Q = Q_\ell$ *at each iteration obtained from the previous solution as in (20). If the initial distribution* Q_0 *satisfies the strict inequality (26) for (1) then*

$$E_c(R, Q_\ell) = E_c^{ML}(R, Q_\ell) \overset{\ell \to \infty}{\searrow} 0.$$

Proof: From (26) follows $C\big(\text{supp}(Q_0)\big) \geq R$. Then Lemma 10 applies and the claim follows by Lemma 6. □

IV. Comparison to the Blahut Algorithm

The fixed-rate iterative computation of the optimal correct-decoding exponent (18) according to (3) and (20) can be compared to the fixed-distortion version of the Blahut algorithm [6], [7] for the rate-distortion function computation. As we have seen from (3), (1), and (18), the optimal correct-decoding exponent can be written as a double minimum, quite similarly to the rate-distortion function:

$$0 = \min_{Q(x)} \min_{\substack{T(y),\, V(x \mid y): \\ \sum_{x,y} T(y)V(x \mid y) \log \frac{V(x \mid y)}{Q(x)} \geq R}} D(T \circ V \parallel Q \circ P), \tag{27}$$

$$R(D) = \min_{Q(x)} \min_{\substack{V(x \mid y): \\ \sum_{x,y} T(y)V(x \mid y)\, d(y, x) \leq D}} D(T \circ V \parallel Q \times T), \tag{28}$$

where in (27) the optimal correct-decoding exponent $E_c(R) = 0$ (implying $R \leq C$). The rate-distortion function $R(D)$ in (28) has also a meaning of an optimal probability exponent [4]. In (28), the discrete memoryless source is denoted as $T(y)$. The i.i.d. source reproduction distribution is denoted as $Q(x)$. The additive distortion measure is $d(y, x)$.

The iterative computation in the two algorithms is, respectively,

$$Q_{\ell+1}(x) = \sum_y \check{T}_\ell(y)\check{V}_\ell(x \mid y), \tag{29}$$

$$Q_{\ell+1}(x) = \sum_y T(y)\, \check{V}_\ell(x \mid y). \tag{30}$$

The algorithm for $R(D)$ is an alternating minimization procedure of Csiszár and Tusnády [7]. That is, in (28), $\check{V}_\ell(x \mid y)$ solves the inner minimum of $D(T \circ V \parallel Q_\ell \times T)$, and then $Q_{\ell+1}(x)$ of (30) in turn minimizes $D(T \circ \check{V}_\ell \parallel Q \times T)$. On the other hand, the proposed algorithm for the correct-decoding exponent is *not* exactly an alternating minimization procedure. Specifically, observe that, in (27), $\check{T}_\ell(y)\check{V}_\ell(x \mid y)$ solves the inner minimum of $D(T \circ V \parallel Q_\ell \circ P)$, but then $Q_{\ell+1}(x)$ of (29) minimizes simultaneously both $D\big(\check{T}_\ell \circ \check{V}_\ell \parallel Q \circ P\big)$ and $D\big(\check{T}_\ell \circ \check{V}_\ell \parallel \check{T}_\ell \times Q\big)$, thus violating the condition under the inner minimum with the same $\check{T}_\ell \circ \check{V}_\ell$. Nonetheless, this results in a monotonically non-increasing sequence of the inner minima over $T \circ V$ at least given the condition on Q_0 of Lemma 10. The sequence converges all the way down to zero at least under the initial condition (26) according to Theorem 2.

In the iterative minimization procedure at fixed rate R described above, the minimization itself is implicit and the slope parameter ρ is different in each iteration. In [9] we present also a fixed-slope version of the iterative update (20), which is similar to the fixed-slope version of the Blahut algorithm for $R(D)$ computation [6], [10], and presents an alternative for the Arimoto algorithm [2] for computation of $\min_Q E_0(\rho, Q)$, $\rho \in (-1, 0)$. There, the slope parameter ρ is fixed and the computations acquire an explicit form, going iteratively along (10)-(11) and (20). Similarly as the Blahut and the Arimoto algorithms, it does not require any special conditions for convergence.

V. Channel Input Adaptation

As we have seen, the correct-decoding exponent for channels exhibits properties reminiscent of the rate-distortion function for sources. In [4], the phenomenon of natural type selection in lossy source-*encoding* was found to be a stochastic counterpart of the Blahut algorithm. In this section we describe an analogous phenomenon in noisy-channel *decoding* as a stochastic counterpart of the fixed-rate iterative minimization of the correct-decoding exponent presented in Section III.

A. Adaptation Scheme

The communication scheme, whose target is to adapt itself to an unknown DMC channel, can employ any sequence (in the blocklength n) of decoders operating on random block codes generated i.i.d. according to Q, resulting in an asymptotic *error* exponent denoted as $E_e(R, Q)$. The communication occurs at a rate R and we assume it to be reliable:

$$E_e(R, Q) > 0.$$

The decoder determines its estimate $\widehat{m}$ of the transmitted message and then sends reliably a bit of feedback, $F = 0$ or 1, to the transmitter, according to the following rule (Figure 3):

$$D(T \circ V_{\widehat{m}} \,\|\, T \times Q) > R + \Delta \quad\Longleftrightarrow\quad F = 1, \tag{31}$$

where $T(y)$ is the type of the received block $\mathbf{y}$, $V_{\widehat{m}}(x \mid y)$ represents the conditional type of the codeword $\mathbf{x}_{\widehat{m}}$ given the received block, and $\Delta > 0$ is some predetermined parameter of the adaptation. This feedback rule corresponds to a boolean function $F : \mathcal{X}^n \times \mathcal{Y}^n \to \{0, 1\}$.

Let $(\mathbf{X}, \mathbf{Y})$ denote the random pair of the transmitted and the received blocks. Define an event:

$$\mathcal{S} \triangleq \Big\{(\mathbf{X}, \mathbf{Y}) \text{ of any type } T \circ V \text{ s.t. } D(T \circ V \,\|\, T \times Q) > R + \Delta\Big\}. \tag{32}$$

Lemma 11 (Selection exponent): If $R + \Delta < R^{-}_{-1}(Q)$, as defined in (14), then

$$\lim_{n\to\infty} \frac{\log \Pr\{\mathcal{S}\}}{-n} = E_c(R + \Delta, Q).$$

Proof: The $\liminf$ of the exponent of $\mathcal{S}$ is lower-bounded by $E_c(R + \Delta, Q)$ defined by (3). Given that $R + \Delta < R^{-}_{-1}(Q)$, by the explicit expression for $E_c(R, Q)$ (16) of Lemma 4 we conclude that $E_c(R + \Delta, Q)$ is continuous at R as a convex ($\cup$) function. This fact can be used for the upper bound. For a small enough $\epsilon > 0$ consider the minimizing solution $T^* \circ V^*$ of $E_c(R + \Delta + 2\epsilon, Q)$. Let $T^*_n \circ V^*_n$ denote a quantized version of $T^* \circ V^*$ with precision $\frac{1}{n}$. Then $T^*_n \circ V^*_n$ is a joint type with denominator n. By continuity of the divergence, for sufficiently large n we obtain $D\big(T^*_n \circ V^*_n \,\|\, T^*_n \times Q\big) \geq R + \Delta + \epsilon$ and also $D\big(T^*_n \circ V^*_n \,\|\, Q \circ P\big) \leq E_c(R + \Delta + 2\epsilon, Q) + \epsilon$. Therefore, the $\limsup$ of the exponent of $\mathcal{S}$ is upper-bounded by $\lim_{\epsilon\to 0} E_c(R + \Delta + 2\epsilon, Q) + \epsilon = E_c(R + \Delta, Q)$. □

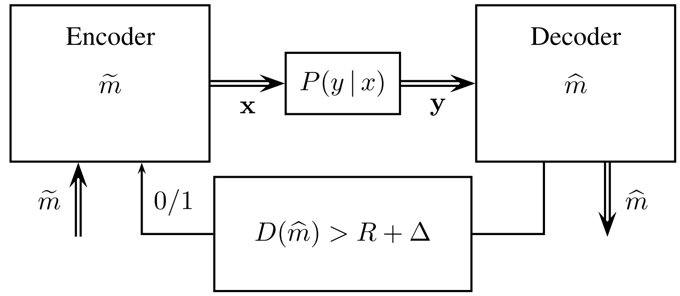

Fig. 3. Channel with a 1-bit feedback per block. The decoder providing $\widehat{m}$ is not specified. It is assumed that the decoding is correct, i.e. $\widehat{m} = \widetilde{m}$. $D(\widehat{m}) \triangleq D(T \circ V_{\widehat{m}} \,\|\, T \times Q)$, where T is the type of the received block, $V_{\widehat{m}}$ is the conditional type of the codeword for the estimated message $\widehat{m}$, and Q is the i.i.d. codebook generating distribution.

The two events $\{F = 1\}$ and $\mathcal{S}$ are of course not the same, because in case of a decoding error the decoded codeword $\mathbf{x}_{\widehat{m}}$ is different from the transmitted codeword $\mathbf{x}_{\widetilde{m}}$. In order to ensure that the two events are the same with high probability, we further assume that Δ is small enough so that

$$E_e(R, Q) > E_c(R + \Delta, Q). \tag{33}$$

Under this condition and the condition of Lemma 11 that $R + \Delta < R^{-}_{-1}(Q)$, given $\mathcal{S}$ with high probability holds also the event $\{F = 1\}$ and vice versa. Given the condition of Lemma 11, $E_c(R+\Delta, Q)$ is the same as the correct-decoding exponent of the ML decoder $E_c^{ML}(R + \Delta, Q)$ according to Lemma 4. This situation is depicted in Figure 4. There, on the upper graph $E_e(R, Q) > E_c(R + \Delta, Q) = 0$, while on the lower graph $E_e(R, Q) > E_c(R + \Delta, Q) > 0$.

In the case $F = 1$, which is a rare event when $E_c(R+\Delta, Q) > 0$, the system parameter Q is updated. A new codebook is adopted by both the encoder and the decoder according to the type of the transmitted codeword $\mathbf{x}_{\widetilde{m}}$:

$$Q'(x) = T_{\widetilde{m}}(x) = T_{\widehat{m}}(x),$$

where $T_m(x) = \sum_y T(y) V_m(x \mid y)$. Under the condition (33) and the condition of Lemma 11, the type of the transmitted codeword is known at the decoder with high probability also given the event $\{F = 1\}$. In case of the feedback $F = 0$, the codebook distribution Q remains unchanged. To summarize:

Feedback	Encoder	Decoder
$F = 1$	$Q(x) \leftarrow T_{\widetilde{m}}(x)$	$Q(x) \leftarrow T_{\widehat{m}}(x)$
$F = 0$	−	−

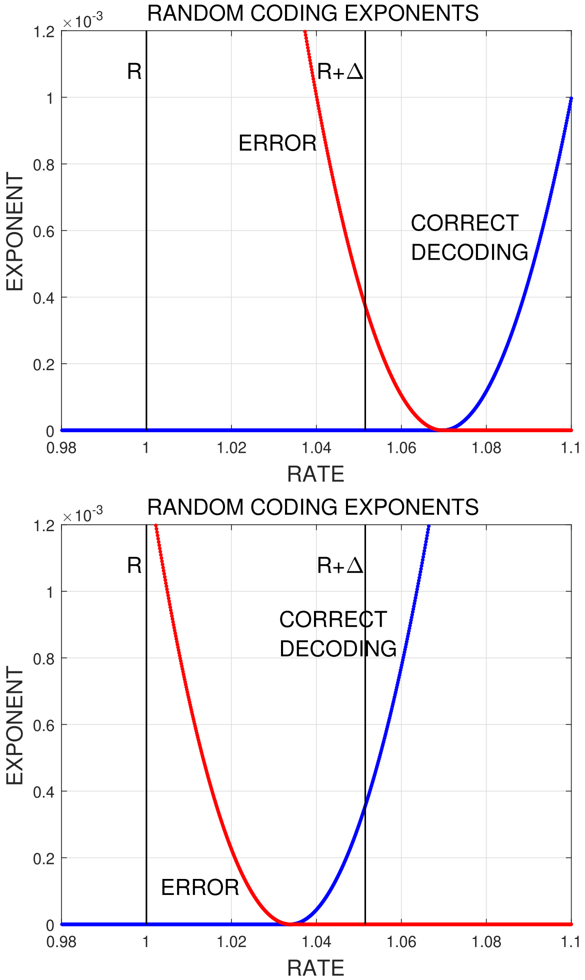

Fig. 4. The decreasing curve is the error exponent $E_e(\widetilde{R}, Q)$. The increasing curve is the correct-decoding exponent $E_c(\widetilde{R}, Q)$. Both graphs are for the same $Q(x)$. The channel $P(y \,|\, x)$ is different between the upper graph and the lower graph. In both cases $E_e(R, Q) > E_c(R + \Delta, Q)$.

A state-machine description of the above scheme can be found in Appendix D.

B. Natural Type Selection

The joint type $T(y)V_{\widetilde{m}}(x \,|\, y)$ of the transmitted and the received blocks given the event $\{F = 1\}$ or $\mathcal{S}$ is related to the probability exponent of this event $E_c(R + \Delta, Q)$.

Theorem 3 (Convergence of a type):
If $R+\Delta < R^{-}_{-1}(Q)$, as defined in (14), then, given the event $\mathcal{S}$ (32), the joint type of the transmitted and the received words $(\mathbf{X}, \mathbf{Y})$ converges in probability, as the blocklength $n \to \infty$, to the minimizing distribution of $E_c(R + \Delta, Q)$ (3).

Proof: By the preceding Lemma 11 the exponent of $\mathcal{S}$ is given by $E_c(R + \Delta, Q)$. Therefore by (16) it is finite. On the other hand, for some $\epsilon > 0$, the exponent in the probability of the event

$$\mathcal{H} \;\triangleq\; \Big\{(\mathbf{X}, \mathbf{Y}) \;\text{ of any type }\; T \circ V \;\; \text{s.t.}\;\; D(T \circ V \,\|\, Q \circ P) \;>\; E_c(R + \Delta, Q) + \epsilon\Big\},$$

is obviously lower-bounded by $E_c(R+\Delta, Q)+\epsilon$. Then, given $\mathcal{S}$ with high probability holds also $\mathcal{S} \cap \mathcal{H}^c$.

Now consider the joint type $T \circ V$ of $(\mathbf{X}, \mathbf{Y})$ given $\mathcal{S} \cap \mathcal{H}^c$. Since $R + \Delta < R^{-}_{-1}(Q)$ by Lemma 4 there exists some $\beta \in (-1, 0]$ such that

$$E_c(R + \Delta, Q) \;=\; E_0(\beta, Q) - \beta(R + \Delta).$$

We can use this β to write

$$\begin{aligned}
E_c(R + \Delta, Q) + \epsilon \;&\overset{\mathcal{H}^c}{\geq}\; D(T \circ V \,\|\, Q \circ P) \\
\overset{\mathcal{S}}{\geq}\;& D(T \circ V \,\|\, Q \circ P) \;-\; \beta \underbrace{\big[R + \Delta - D(T \circ V \,\|\, T \times Q)\big]}_{\leq 0} \\
=\;& D(T \,\|\, T_\beta) \;+\; (1+\beta) D(T \circ V \,\|\, T \circ V_\beta) \;+ \\
& \underbrace{E_0(\beta, Q) \;-\; \beta(R + \Delta)}_{E_c(R+\Delta,\, Q)} \\
=\;& D(T \,\|\, T_\beta) \;+\; (1+\beta) D(T \circ V \,\|\, T \circ V_\beta) \;+ \\
& E_c(R + \Delta, Q) \\
\epsilon \;\geq\;& D(T \,\|\, T_\beta) \;+\; (1+\beta) D(T \circ V \,\|\, T \circ V_\beta),
\end{aligned} \tag{34}$$

where $T_\beta \circ V_\beta$ is the minimizing distribution of $E_c(R+\Delta, Q)$ determined according to Lemma 4 by (10)-(11) with β. The inequality (34) implies that the type $T \circ V$ and the solution $T_\beta \circ V_\beta$ are close in $\mathcal{L}_1$ norm. And all this — given $\mathcal{S} \cap \mathcal{H}^c$, i.e. with high probability. □

In the subsequent analysis we assume that the blocklength n is large and neglect the difference between the random joint type of the transmitted and the received blocks $T(y)V_{\widetilde{m}}(x \,|\, y)$ given $\{F = 1\}$ and the respective solution $\check{T}(y)\check{V}(x \,|\, y)$ to the minimization problem (3) $E_c(R + \Delta, Q)$ or (1) $E_c^{ML}(R + \Delta, Q)$. We also assume that the inequality (33) between the error exponent and the correct-decoding exponent is never violated, so that $\{F = 1\}$ is always exponentially equivalent in probability to $\mathcal{S}$.

Let Q_0 be the initial codebook distribution and consider the consecutive events $\big\{\mathcal{S}_\ell\big\}_{\ell=0}^{+\infty}$, defined by (32). They result in the sequence of codebook distributions $\big\{Q_\ell\big\}_{\ell=1}^{+\infty}$. Suppose that initially

$$C\big(\text{supp}(Q_0)\big) \;>\; R + \Delta.$$

Then by Lemma 8 it is also true that $R + \Delta < R^{-}_{-1}(Q_0)$, which is the condition of both Lemma 11 and Theorem 3. As a result, given (33) for Q_0 the events $\{F = 1\}$ and $\mathcal{S}$ are equivalent and given these events the joint type of the transmitted and the received blocks (approximately, with high probability) achieves the minima $E_c(R + \Delta, Q_0)$ and $E_c^{ML}(R+\Delta, Q_0)$, with $E_c(R+\Delta, Q_0) = E_c^{ML}(R+\Delta, Q_0)$. Therefore the next distribution Q_1 is obtained according to (19)-(20). Finally Lemma 9 gives $\text{supp}(Q_1) = \text{supp}(Q_0)$. Then, provided that (33) continues to hold for each Q_ℓ, by induction we obtain that at each iteration ℓ the codebook distribution $Q_{\ell+1}$ evolves according to (19)-(20). This results in convergence of $E_c^{ML}(R + \Delta, Q_\ell)$. Suppose the initial distribution Q_0 satisfies further the strict inequality (26) with $R + \Delta$ in place of R:

$$E_c^{ML}(R + \Delta, Q_0) \;<\; \min_{Q:\; C(\text{supp}(Q)) \,<\, R + \Delta} E_c^{ML}(R + \Delta, Q). \tag{35}$$

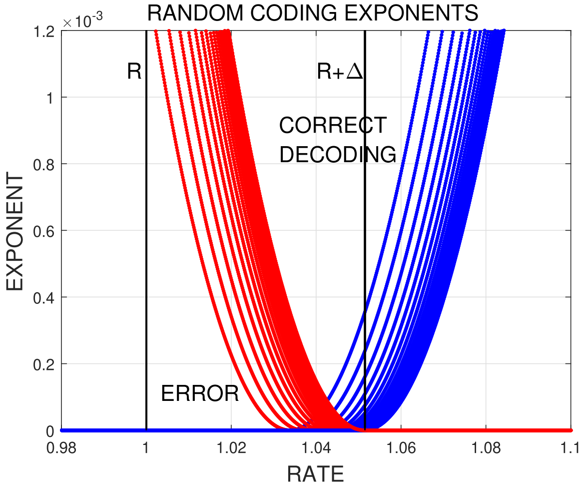

Fig. 5. The decreasing curves are the error exponents $E_e(\widetilde{R}, Q_\ell)$. The increasing curves are the correct-decoding exponents $E_c(\widetilde{R}, Q_\ell)$. All the curves are for the same channel $P(y\,|\,x)$. For each $\ell = 0, 1, 2, \ldots$, the respective pair of curves meets zero at the same point $\widetilde{R} = I(Q_\ell, P)$. For each ℓ holds $E_e(R, Q_\ell) > E_c(R+\Delta, Q_\ell)$ (33). The correct-decoding exponent $E_c(R+\Delta, Q_\ell)$ converges to zero as ℓ grows. At the same time the zero point of the error exponent at $\widetilde{R} = I(Q_\ell, P)$ moves to the right towards $R+\Delta$.

This is always possible with $C\big(\text{supp}(Q_0)\big) > R+\Delta$. Then the sequence of $E_c^{ML}(R+\Delta, Q_\ell)$ converges to zero by Lemma 6, achieving our goal. In the limit of convergence of the codebook distribution for a given channel — reliable communication is possible for all rates below $R+\Delta$.

An example is shown in Figures 4 and 5.

In Figure 4 on the upper graph the correct-decoding exponent is zero at $R+\Delta$. The rate of the communication is lower and equals R. Then the channel $P(y\,|\,x)$ changes abruptly and both the error exponent curve and the correct-decoding exponent curve for the same $Q(x)$ move to the left, as shown on the lower graph of Figure 4. Now the correct-decoding exponent becomes positive at $R+\Delta$, but is still lower than the error exponent at R, so that the strict inequality (33) still holds. The reliable communication continues at R. The new channel $P(y\,|\,x)$ is assumed to remain *the same* during the ensuing iterations, shown in Figure 5. During the iterations the codebook distribution adapts to the new channel. In the limit of the iterations, the correct-decoding exponent returns to zero at $R+\Delta$ with respect to the new channel. In this way the adaptation scheme will safeguard the reliable communication mode at R for as long as the DMC capacity of the block does not deteriorate below $R+\Delta$.

In the presented example the change in the channel is abrupt relatively to the number of block transmissions required to adapt to the change. If we increase Δ, then $R+\Delta$ will move to the right in the graphs and the correct-decoding exponent at $R+\Delta$ will be accordingly higher. The higher is this exponent — the more blocks we have to wait in order for a single iteration to occur.

In practice, the correct-decoding exponent at $R+\Delta$ should be near zero and the change in the channel should be slow, in order for the scheme to be able to follow the changes in the channel successfully. In the tracking scenario, if the parameter Δ is such that the correct-decoding exponent is initially zero at $R+\Delta$, then the higher is Δ — the greater is the communication reliability at R. On the other hand, the higher is Δ — the higher must be the gap to capacity and the allowed region for the change of the capacity itself is more restricted from below. It should be noted, that since the reliable communication never occurs exactly at the capacity, in the reliable communication mode there always should exist some $\Delta > 0$ to work with.

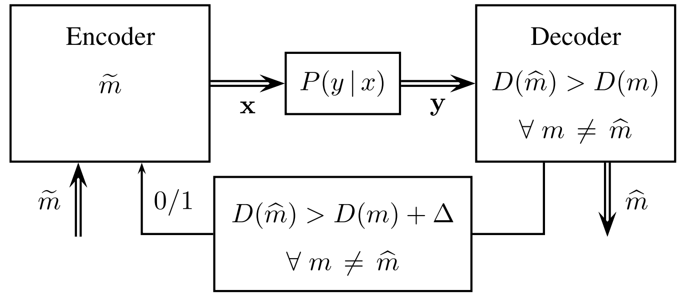

Fig. 6. An alternative scheme. $D(m) \triangleq D(T \circ V_m \,\|\, T \times Q)$, where T is the type of the received block, V_m is the conditional type of the codeword for the message m, and Q is the i.i.d. codebook generating distribution.

C. Alternative Scheme

The adaptation scheme presented in Figure 6 is embedded in the structure of a particular channel-decoding procedure through the parameter of decoding confidence $\Delta > 0$. Maintaining or restoring the decoding confidence means adaptation. In this scheme the decoder itself uses the channel-independent metric

$$\log \frac{V_m(x\,|\,y)}{Q(x)}, \tag{36}$$

introduced in [12], where $V_m(x\,|\,y)$ is the conditional type of the codeword for message m given the received block. The decoder searches for the maximal empirical average of this metric among the codewords in the codebook. If only a single codeword attains the maximum, the decoder then compares the difference between the maximal empirical average of (36) and the second highest one in the codebook to the parameter Δ. If the winning codeword wins by more than Δ, its empirical distribution is selected as the new codebook distribution.

It can be shown [9] that in this scheme the exponent of the type selection event is also given by $E_c(R+\Delta, Q)$ defined in (3), so it works equivalently to the scheme in Figure 3.

On the other hand, it can be shown [9] that the exponent of the complementary non-selection event in this scheme is given by

$$E_e(R+\Delta, Q) = \min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \,\|\, Q \circ P) + \big|D(T \circ V \,\|\, T \times Q) - R - \Delta\big|^{+} \Big\}, \tag{37}$$

where the minimization is over arbitrary distributions $T(y)V(x\,|\,y)$, with $y \in \mathcal{Y}$ and $x \in \mathcal{X}$. This is the exponent of the event when the transmitted codeword does not win by Δ. It can be shown [1], [9], that (37) is just the Gallager random coding error exponent [3, eq. 5.6.28] shifted by Δ.

VI. Conclusion

In this work we introduce two different expressions (18) for the optimal correct-decoding exponent:

$$E_c(R) = \min_{Q(x)} \min_{T(y),\, V(x\,|\,y)} \Big\{ D(T\circ V \,\|\, Q\circ P) + \big|R - D(T\circ V \,\|\, T\times Q)\big|^+ \Big\} \quad (38)$$

$$\equiv \min_{Q(x)} \min_{\substack{T(y),\, V(x\,|\,y):\\ D(T\circ V \,\|\, T\times Q)\,\geq\, R}} \Big\{ D(T\circ V \,\|\, Q\circ P) \Big\}, \quad (39)$$

as alternatives to the Dueck-Körner expression [8]. The inner minimum in (38) has a meaning of the correct-decoding exponent of the ML decoder for a given i.i.d. codebook distribution Q. We propose a minimization procedure over Q at constant R, which uses the inner minimum in (38) iteratively. It is shown that this procedure results in a sequence of distributions Q_ℓ with a monotonically non-increasing sequence of the corresponding inner minima in (38). This sequence of minima converges eventually to the outer minimum in (38) over some subset of the channel input alphabet, and more precisely — over some *subset* of the support $\text{supp}(Q_0)$ of the initial distribution Q_0. In general, it remains unclear whether the minimization procedure at constant R *always* achieves the global minimum (38) over the initial channel input support $\text{supp}(Q_0)$ itself. If we knew that it does, we could use any initial channel input distribution Q_0 which is positive everywhere — as in the Arimoto-Blahut algorithms.

From a practical standpoint, it is interesting when the correct-decoding exponent is zero. This is when reliable communication becomes possible. For any rate R below the capacity, we provide a minimal and quite obvious sufficient condition (26) on the initial distribution Q_0, which guarantees convergence of the minimization procedure to zero. This sufficient condition is always satisfied, for example, for a binary channel-input alphabet, and for greater alphabets presents an inner bound on the region of convergence of the fixed-rate computation algorithm in terms of Q_0 for each rate below the capacity. This "computation of zero" is interesting, of course, only because of the unknown set of the distributions Q, achieving zero correct-decoding exponent for a given R.

The inner minima in (38) and (39) coincide, as increasing functions of R, for slopes less than 1. This coincidence allows us to give a stochastic interpretation to the fixed-rate minimization procedure and to propose a scheme for the channel input adaptation (Figures 3 and 6). The scheme does not rely on the knowledge of the channel. In this scheme the communication occurs at a rate R and is assumed sufficiently reliable from the beginning of the adaptation. Then, in the limit of a large blocklength, the adaptation falls exactly into the steps of the iterative minimization procedure. As a result, under the initial condition (35) the ML correct-decoding exponent, associated with the iterated input distribution Q_ℓ, gradually descents to zero at $R+\Delta$, thereby securing the reliable communication mode at R.

The adaptation scheme uses a single bit of feedback per transmitted block. According to this bit the system decides whether to replace the codebook distribution Q with the empirical distribution of the last sent codeword or not. In practice, a less interesting case would be when the feedback bit has entropy zero, i.e. when the feedback bit is 1 or 0 with high probability. The first situation occurs when the ML correct-decoding exponent curve for a given Q leaves zero at a point on the rate-axis substantially greater than $R+\Delta$, i.e., the system is deep inside the region of reliable communication (Figure 4, upper graph). Then the feedback bit is 1 with high probability. In this case there is no clear advantage of the selected empirical distribution over Q and its constant replacement is not vital. The second situation happens when the correct-decoding exponent is substantially positive at $R+\Delta$ (Figure 4, lower graph). In this case, the feedback bit is 0 with high probability, and it naturally takes an exponentially large number of blocks to obtain a single adaptation step.

Therefore, the promising case seems to be in the transition zone, when the feedback bit has a non-zero entropy. This is the situation when the correct-decoding exponent meets zero at $R+\Delta$ (as in the limit of the iterations in Figure 5) and fluctuates there, at a finite blocklength, rising up following the changes in the channel and falling back to zero as a result of the adaptation process. For such fluctuations, the sufficient condition (35) is adequate and enough, because it stays satisfied. The choice of Δ for a given R then amounts to a trade-off between the communication reliability and allowed variability of the channel capacity, as discussed earlier, in the end of Section V-B. The question however remains for future research — how slow and how large, respectively, the change in the channel and the size of the block have to be in order for the adaptation mechanism to follow the channel from block to block.

Appendix

A. Proof of Lemma 1

If the LHS of (5) is $+\infty$, then (5) holds with strict inequality, because the RHS of (5) is always finite. Otherwise we can write:

$$\min_{\substack{T(y),\, V(x\,|\,y):\\ D(T\circ V \,\|\, T\times Q)\,\geq\, R}} \Big\{ D(T\circ V \,\|\, Q\circ P) \Big\} = \quad (40)$$

$$\overset{(a)}{=} D\big(T_R\circ V_R \,\|\, Q\circ P\big) \quad (41)$$

$$\overset{(b)}{\geq} D\big(T_R\circ V_R \,\|\, Q\circ P\big) + \rho\underbrace{\Big[D\big(T_R\circ V_R \,\|\, T_R\times Q\big) - R\Big]}_{\leq 0} \quad (42)$$

$$\overset{(c)}{\geq} \min_{\substack{T(y),\, V(x\,|\,y):\\ \text{supp}(V)\,\subseteq\,\text{supp}(Q)}} \Big\{ D(T\circ V \,\|\, Q\circ P) + \rho\Big[D(T\circ V \,\|\, T\times Q) - R\Big]\Big\} \quad (43)$$

$$\overset{(d)}{=} D\big(T_\rho\circ V_\rho \,\|\, Q\circ P\big) + \rho\Big[D\big(T_\rho\circ V_\rho \,\|\, T_\rho\times Q\big) - R\Big]$$

$$\overset{(e)}{=} D\big(T_\rho\circ V_\rho \,\|\, Q\circ P\big)$$

$$\overset{(f)}{\geq} \min_{\substack{T(y),\, V(x\,|\,y):\\ D(T\circ V \,\|\, T\times Q)\,\geq\, R}} \Big\{ D(T\circ V \,\|\, Q\circ P) \Big\}.$$

When the minimum (40) is finite, the first equality (a) above holds, with $T_R \circ V_R$ denoting a minimizing solution of (40) for a given R. The inequality (b) holds because $\rho \leq 0$ and $D\big(T_R \circ V_R \parallel T_R \times Q\big) \geq R$. The inequality ($c$) holds because $D\big(T_R \circ V_R \parallel Q \circ P\big)$ is finite, so that $\text{supp}(V_R) \subseteq \text{supp}(Q)$. In the second equality (d) above, $T_\rho \circ V_\rho$ denotes a minimizing solution of the minimum (43) for a given ρ.

For the direct part, observe that when the minima (40) and (43) are equal, then also there is equality between the expression (42) and the minimum (43). Consequently, the minimizing distribution of (40) $T_R \circ V_R$ is also a minimizing distribution of (43) for a given ρ in this case. From the equality between (41) and (42) we conclude that such solution must satisfy $R = D\big(T_R \circ V_R \parallel T_R \times Q\big)$ for $\rho < 0$, or, as a solution to (40), it can be such that $R \leq D\big(T_R \circ V_R \parallel T_R \times Q\big)$ for $\rho = 0$.

Conversely, observe that if $R = D\big(T_\rho \circ V_\rho \parallel T_\rho \times Q\big)$, or $R \leq D\big(T_0 \circ V_0 \parallel T_0 \times Q\big)$ for $\rho = 0$, then both (e) and (f) hold. In this case the minimum (40) is finite and (a)-(c) also hold. By the sandwich, we conclude that there is equality between (40) and (43). Moreover, since also $D\big(T_\rho \circ V_\rho \parallel Q \circ P\big)$ is equal to the minimum (40), and since $R \leq D\big(T_\rho \circ V_\rho \parallel T_\rho \times Q\big)$, we conclude that $T_\rho \circ V_\rho$ is also a minimizing solution of (40). □

B. Proof of Lemma 2

Similarly to Lemma 1:

$$\min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \parallel Q \circ P) + \big|R - D(T \circ V \parallel T \times Q)\big|^+ \Big\} \tag{44}$$

$$\overset{(a)}{=} D\big(T_R \circ V_R \parallel Q \circ P\big) \;+\; \big|R - D\big(T_R \circ V_R \parallel T_R \times Q\big)\big|^+$$

$$\overset{(b)}{\geq} D\big(T_R \circ V_R \parallel Q \circ P\big) \;-\; \rho\,\big[R - D\big(T_R \circ V_R \parallel T_R \times Q\big)\big]$$

$$\overset{(c)}{\geq} \min_{\substack{T(y),\, V(x\,|\,y): \\ \text{supp}(V) \subseteq \text{supp}(Q)}} \Big\{ D(T \circ V \parallel Q \circ P) - \rho\,\big[R - D(T \circ V \parallel T \times Q)\big] \Big\} \tag{45}$$

$$\overset{(d)}{=} D\big(T_\rho \circ V_\rho \parallel Q \circ P\big) \;-\; \rho\,\big[R - D\big(T_\rho \circ V_\rho \parallel T_\rho \times Q\big)\big]$$

$$\overset{(e)}{=} D\big(T_\rho \circ V_\rho \parallel Q \circ P\big) \;+\; \big|R - D\big(T_\rho \circ V_\rho \parallel T_\rho \times Q\big)\big|^+$$

$$\geq \min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \parallel Q \circ P) + \big|R - D(T \circ V \parallel T \times Q)\big|^+ \Big\}.$$

In (a) $T_R \circ V_R$ denotes a minimizing solution of (44) for a given R, (b) always holds with $-1 \leq \rho \leq 0$, (c) holds because $T_R \circ V_R$ has to be such that $D\big(T_R \circ V_R \parallel Q \circ P\big)$ is finite, giving $\text{supp}(V_R) \subseteq \text{supp}(Q)$, in ($d$) $T_\rho \circ V_\rho$ denotes a minimizing solution of the minimum (45) for a given ρ. If $R = D\big(T_\rho \circ V_\rho \parallel T_\rho \times Q\big)$, or $R \leq D\big(T_0 \circ V_0 \parallel T_0 \times Q\big)$ for $\rho = 0$, or $R \geq D\big(T_{-1} \circ V_{-1} \parallel T_{-1} \times Q\big)$ for $\rho = -1$, then (e) holds. The rest of the argument is analogous to the proof of Lemma 1. □

C. Proof of Lemma 3

For $\rho > -1$:

$$\begin{aligned}
&\min_{T(y),\, V(x\,|\,y)} \Big\{ D(T \circ V \parallel Q \circ P) \;+\; \rho D(T \circ V \parallel T \times Q) \Big\} \\
&= \min_{T(y),\, V(x\,|\,y)} \Big\{ \underbrace{D(T \parallel T_\rho)}_{\geq 0} + (1+\rho)\, \underbrace{D(T \circ V \parallel T \circ V_\rho)}_{\geq 0} \Big\} \\
&\quad + E_0(\rho, Q) \qquad\qquad (46)\\
&= E_0(\rho, Q),
\end{aligned}$$

where the unique joint distribution minimizing the divergences in (46) is $T_\rho \circ V_\rho$ given by (10)-(11).

For $\rho = -1$:

$$\begin{aligned}
&\min_{\substack{T(y),\, V(x\,|\,y): \\ \text{supp}(V) \subseteq \text{supp}(Q)}} \Big\{ D(T \circ V \parallel Q \circ P) - D(T \circ V \parallel T \times Q) \Big\} \\
&= \min_{\substack{T(y),\, V(x\,|\,y): \\ \text{supp}(V) \subseteq \text{supp}(Q)}} \Big\{ \sum_{x,\, y} T(y) V(x\,|\,y) \log \frac{T(y)}{P(y\,|\,x)} \Big\} \\
&= \min_{T(y)} \Big\{ \underbrace{D(T \parallel T_{-1})}_{\geq 0} \Big\} \;+\; E_0(-1, Q) \\
&= E_0(-1, Q),
\end{aligned}$$

where the minimum is achieved with any $V(x\,|\,y)$ satisfying (13) and the unique $T_{-1}(y)$ given by (12). □

D. A State-Machine Description of the Adaptation System

Assuming the decoding is always correct: $\widehat{m} = \widetilde{m}$, the codebook distribution Q can be considered as a state of the whole system, which may change in time, i.e. from block to block. But strictly speaking, it may be different at the receiver than at the transmitter. Let $t = 1, 2, 3, \ldots$ be a time index, corresponding to the current block. With the help of this index, let us denote the current codebook distribution, or the state, as $Q^{(t)}$ at the transmitter and as $\widehat{Q}^{(t)}$ at the receiver. Using the same codebook distribution $Q^{(t)}$, the codebook itself, however, is generated independently, i.e. differently, at different times t. This can be assumed to simplify the analysis. We assume that the codebooks on both sides at time t are exactly the same if $Q^{(t)} = \widehat{Q}^{(t)}$. Therefore, the codebooks used by the transmitter and the receiver can be viewed as functions of the time index t and the current codebook distribution $Q^{(t)}$ or $\widehat{Q}^{(t)}$, respectively.

On the transmitter side, accordingly, the transmitted codeword $\mathbf{x}^{(t)} \in \mathcal{X}^n$ at time t can be viewed as a function of the current transmitted message $\widetilde{m}^{(t)}$, of the current time t, and the current codebook distribution $Q^{(t)}$:

$$\mathbf{x}^{(t)} \;=\; \text{enc}\big(\widetilde{m}^{(t)},\, t,\, Q^{(t)}\big). \tag{47}$$

At time t, the encoder also determines its next codebook distribution $Q^{(t+1)}$, according to the feedback bit $F^{(t)} \in \{0, 1\}$ at that time and the type of the transmitted codeword $\mathbf{x}^{(t)}$. The next state $Q^{(t+1)}$ at the encoder can be described alternatively as a function of $F^{(t)}$, $\widetilde{m}^{(t)}$, t, and its current state $Q^{(t)}$:

$$Q^{(t+1)} \;=\; (1 - F^{(t)}) \cdot Q^{(t)} + F^{(t)} \cdot \text{type}\big(\widetilde{m}^{(t)},\, t,\, Q^{(t)}\big), \tag{48}$$

where type $\left(\widetilde{m}^{(t)},\, t,\, Q^{(t)}\right)$ is a function, which gives the type of the codeword $\mathbf{x}^{(t)}$.

The decoder uses the current received block $\mathbf{y}^{(t)} \in \mathcal{Y}^n$, the current time t, and its current state $\widehat{Q}^{(t)}$ to determine its estimate of the transmitted message $\widehat{m}^{(t)}$ and the feedback bit $F^{(t)}$:

$$\widehat{m}^{(t)} \;=\; \mathrm{dec}\left(\mathbf{y}^{(t)},\, t,\, \widehat{Q}^{(t)}\right), \tag{49}$$

$$F^{(t)} \;=\; \mathrm{bit}\left(\mathbf{y}^{(t)},\, t,\, \widehat{Q}^{(t)}\right). \tag{50}$$

The decoder then propagates its own state, using the same function as (48), with the same feedback bit input $F^{(t)}$, but with formally different inputs $\widehat{m}^{(t)}$ and $\widehat{Q}^{(t)}$:

$$\widehat{Q}^{(t+1)} \;=\; (1-F^{(t)})\cdot \widehat{Q}^{(t)} + F^{(t)}\cdot \mathrm{type}\left(\widehat{m}^{(t)},\, t,\, \widehat{Q}^{(t)}\right), \tag{51}$$

where type $\left(\widehat{m}^{(t)},\, t,\, \widehat{Q}^{(t)}\right)$ is the type of the codeword $\mathbf{x}_{\widehat{m}^{(t)}}$ in the codebook determined by t and $\widehat{Q}^{(t)}$.

The initial state $Q^{(1)} = \widehat{Q}^{(1)}$ can be an arbitrary distribution over $\mathcal{X}$, generating the same codebook on both sides. After the first instance of the feedback bit $F^{(t)} = 1$, the states on each side become types (the same type, provided $\widehat{m} = \widetilde{m}$) and after that point in time the total number of different possible states $Q^{(t)}$ or $\widehat{Q}^{(t)}$ is upper-bounded by the total number of different types for the blocklength n, and therefore by $(n+1)^{|\mathcal{X}|}$.

REFERENCES

[1] S. Tridenski and R. Zamir, "Exponential source/channel duality," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 3140–3144.

[2] S. Arimoto, "Computation of random coding exponent functions," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 665–671, Nov. 1976.

[3] R. G. Gallager, *Information Theory and Reliable Communication*. Hoboken, NJ, USA: Wiley, 1968.

[4] R. Zamir and K. Rose, "Natural type selection in adaptive lossy compression," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 99–111, Jan. 2001.

[5] Y. Kochman and R. Zamir, "Adaptive parametric vector quantization by natural type selection," in *Proc. Data Compress. Conf. (DCC)*, Snowbird, UT, USA, Mar. 2002, p. 392.

[6] R. E. Blahut, "Computation of channel capacity and rate-distortion functions," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 460–473, Jul. 1972.

[7] I. Csiszár and G. Tusnády, "Information geometry and alternating minimization procedures," *Statist. Decisions*, Suppl. 1, pp. 205–237, 1984.

[8] G. Dueck and J. Körner, "Reliability function of a discrete memoryless channel at rates above capacity (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 1, pp. 82–85, Jan. 1979.

[9] S. Tridenski and R. Zamir, "Channel input adaptation via natural type selection," 2018, *arXiv:1811.01354*. [Online]. Available: https://arxiv.org/abs/1811.01354

[10] I. Csiszár, "On the computation of rate-distortion functions (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 122–124, Jan. 1974.

[11] Y. Oohama and Y. Jitsumatsu, "A new iterative algorithm for computing the optimal exponent of correct decoding for discrete memoryless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 924–928.

[12] N. Merhav, "Reliability of universal decoding based on vector-quantized codewords," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 2696–2709, May 2017.

[13] S. Tridenski and R. Zamir, "Channel input adaptation via natural type selection," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 226–230.

Sergey Tridenski graduated from Belarusian State University, Minsk, Belarus, faculty of radiophysics and electronics, in 1996, received the M.Sc. and Ph.D. degrees in electrical engineering from Tel-Aviv University, Israel, in 2012 and 2019, respectively. He is currently with Bar-Ilan University, Ramat-Gan, Israel.

Ram Zamir was born in Ramat-Gan, Israel in 1961. He received the B.Sc., M.Sc. (summa cum laude) and D.Sc. (with distinction) degrees from Tel-Aviv University, Israel, in 1983, 1991, and 1994, respectively, all in electrical engineering. In the years 1994 - 1996 he spent post-doctoral periods at Cornell University, Ithaca, NY, and at the University of California at Santa Barbara. In 2002 he spent a Sabbatical year at MIT, and in 2008 and 2009 short Sabbaticals at ETH and MIT. Since 1996 he has been with the department of Elect. Eng. - Systems at Tel Aviv University.

Ram Zamir has been consulting in the areas of radar and communications (DSL and WiFi), where he was involved with companies like Orckit and Actelis. During the period 2005-2014 he was the Chief Scientist of Celeno Communications. He has been teaching information theory, data compression, random processes, communications systems and communications circuits at Tel Aviv University. He is an IEEE fellow since 2010. He served as an Associate Editor for Source Coding in the IEEE TRANSACTIONS ON INFORMATION THEORY (2001-2003), headed the Information Theory Chapter of the Israeli IEEE society (2000-2005), and was a member of the BOG of the society (2013-2015). His research interests include information theory (in particular: lattice codes for multi-terminal problems), source coding, communications and statistical signal processing. His book "Lattice coding for signals and networks" was published in 2014.