Proof of Convergence for Correct-Decoding Exponent Computation

Sergey Tridenski  
Faculty of Engineering  
Bar-Ilan University, Israel  
Email: tridens@biu.ac.il

Anelia Somekh-Baruch  
Faculty of Engineering  
Bar-Ilan University, Israel  
Email: somekha@biu.ac.il

Ram Zamir  
EE - Systems Department  
Tel-Aviv University, Israel  
Email: zamir@eng.tau.ac.il

Abstract—For a discrete memoryless channel with finite input and output alphabets, we prove convergence of an iterative computation of the optimal correct-decoding exponent as a function of communication rate, for a fixed rate and for a fixed slope.

I. INTRODUCTION

Consider a standard information theoretic setting of transmission through a discrete memoryless channel (DMC), with finite input and output alphabets, using block codes. For communication rates above capacity, the average probability of correct decoding in a block code tends to zero exponentially fast as a function of the block length. In the limit of a large block length, the lowest possible exponent corresponding to the probability of correct decoding, also called the reliability function above capacity, for all\(^1\) rates \(R \geq 0\) is given by [1]

\[
E_c(R) = \min_{W(y|x)} \left\{ D(W \| P) + |R - I(Q,W)|^+ \right\},
\]

where \(P\) denotes the channel’s transition probability \(P(y | x)\), \(D(W \| P)\) is the Kullback-Leibler divergence between the conditional distributions \(W\) and \(P\), averaged over \(Q\), \(I(Q,W)\) is the mutual information of a pair of random variables with a joint distribution \(Q(x)W(y | x)\), and \(|t|^+ = \max\{0,t\}\).

For certain applications, it is important to be able to know the actual value of \(E_c(R)\) when it is positive. For example, in applications of secrecy, it might be interesting to know the correct-decoding exponent of an eavesdropper. Several algorithms have been proposed for computation of \(E_c(R)\).

In the algorithm by Arimoto [2] the computation of \(E_c(R)\) is facilitated by an alternative expression for it \([3],[1],[4]\):

\[
E_c(R) = \sup_{0 \leq \rho < 1} \min_Q \left\{ E_0(-\rho,Q) + \rho R \right\},
\]

where \(E_0(-\rho,Q)\) is the Gallager exponent function \([6]\), Eq. 5.6.14). In [2], \(\min_Q E_0(-\rho,Q)\) is computed for a fixed slope parameter \(\rho\). The computation is performed iteratively as alternating minimization, based on the property that \(\min_Q E_0(-\rho,Q)\) can be written as a double minimum:

\[
\min_Q \min_V \left\{ - \log \sum_{x,y} Q^{1-\rho}(x)V^\rho(y|x)P(y | x) \right\},
\]

\(^1\)The expression gives zero for the rates \(R \leq \max_Q I(Q,P)\).

where the inner minimum is in fact equal to \(E_0(-\rho,Q)\).
In [4], [5] a different alternating-minimization algorithm is introduced, based on the property, that \(\min_Q E_0(-\rho,Q)\) can be written as another double minimum over distributions:

\[
\min_T \min_{V,T} \left\{ - \sum_{x,y} T(y)V(x | y) \log \frac{V^\rho(x | y)P(y | x)}{U_1Q(x)V(x | y)} \right\},
\]

where \(U_1(x) = \sum_y T_1(y)V_1(x | y)\). As with (3), the computation of \(E_c(R)\) with (4) is also performed for a fixed \(\rho\).

Sometimes, however, it is suitable or desirable to compute \(E_c(R)\) directly for a given rate \(R\). For example, when \(E_c(R) = 0\), and we would like to find such a distribution \(Q\), for which the minimum (1) is zero, as a by-product of the computation. Such distribution \(Q\) has a practical meaning of a channel input distribution achieving reliable communication.

In [7], an iterative minimization procedure for computation of \(E_c(R)\) at fixed \(R\) is proposed, using the property that \(E_c(R)\) can be written as a double minimum \([8]\):

\[
\min_{Q(x)} \min_{T(y)} \left\{ D(TV \| QP) + |R - D(V \| Q) + R| \right\},
\]

where the inner min equals \(\sup_{0 \leq \rho < 1} \{ E_0(-\rho,Q) + \rho R \}\).

In [7], the inner minimum of (5) is computed stochastically by virtue of a correct-decoding event itself, yielding the minimizing solution \(T^*V^*\). The computation is then repeated iteratively, by assigning \(Q(x) = \sum_y T^*(y)V^*(x | y)\).

It is shown in [7, Theorem 1], that the iterative procedure using the inner minimum of (5) leads to convergence of this minimum to the double minimum (5), which is evaluated at least over some subset of the support of the initial distribution \(Q_0\).

In addition, a sufficient condition on \(Q_0\) is provided, which guarantees convergence of the inner minimum in (5) to zero. This condition on \(Q_0\) in [7, Lemma 6] is rather limiting, and is hard to verify.

In the current work, we improve the result of [7]. We modify the method of Csiszár and Tusnády [9] to prove that the iterative minimization procedure of [7] converges to the global minimum (5) over the support of the initial distribution \(Q_0\) itself, for any \(R\) (i.e., not only if the global minimum is zero), and without any additional condition. In particular, use of a strictly positive \(Q_0\) guarantees convergence to \(E_c(R)\).

By a similar method, we also show convergence of the fixed-slope counterpart of the minimization (5), which is
an alternating minimization at fixed $\rho$, based on the double minimum
\[
\min_{Q} \min_{T, V} \left\{ -\sum_{x, y} T(y)V(x \mid y) \log \frac{Q^{1-\rho}(x)P(y \mid x)}{T(y)V^{1-\rho}(x \mid y)} \right\}, \tag{6}
\]
where the inner minimum is in fact equal to $E_0(-\rho, Q)$.

We extend the analysis, presented here, in the full version of the current paper [10]. There, we slightly generalize the expression (5). Using this generalization, we prove convergence of a parametric family of iterative computations, of which the computation according to (4), [4], as well as the computations according to (5) from [7], and according to (6), become special cases.

Besides the variable $R$, we take into account also a possible channel-input constraint, denoted by $\alpha$. In Section II we examine the expression for the correct-decoding exponent. In Section III we prove convergence of the iterative minimization for fixed $(R, \alpha)$. In Section IV we prove convergence of the iterative minimization for fixed gradient w.r.t. $(R, \alpha)$. In Sections V and VI we prove convergence of mixed scenarios: for fixed $\alpha$ and slope $\rho$ in the direction of $R$, and vice versa.

II. CORRECT-DECODING EXPONENT

Let $P(y \mid x)$ denote transition probabilities in a DMC from $x \in \mathcal{X}$ to $y \in \mathcal{Y}$, where $\mathcal{X}$ and $\mathcal{Y}$ are finite channel input and output alphabets, respectively. Suppose also that the channel input satisfies an additive cost function $f(x)$ with an average input constraint $\alpha$, chosen such that $\alpha \geq \min_x f(x)$. The maximum-likelihood correct-decoding exponent ([1], [11]) of this channel, as a function of the rate $R$ and the input constraint $\alpha$, is given by
\[
E_c(R, \alpha) = \min_{Q(x)} \min_{W(y \mid x)} \left\{ D(QW \parallel WP) + \left| R - I(Q, W) \right|^+ \right\}, \tag{7}
\]
where $D(QW \parallel WP)$ denotes the Kullback-Leibler divergence between the joint distributions $Q(x)W(y \mid x)$ and $Q(x)P(y \mid x)$, denoted as $QW$ and $QP$, respectively, and $\mathbb{E}_Q[f(X)]$ denotes the expectation of $f(x)$ w.r.t. the distribution $Q(x)$. The expression (7) can be bounded as follows:
\[
\min_{Q(x)} \min_{W(y \mid x)} \left\{ D(QW \parallel WP) + \left| R - I(Q, W) \right|^+ \right\} \geq \min_{Q(x)} \min_{U(z), W(y \mid z)} \left\{ D(UW \parallel WP) + \left| R - I(U, W) - D(U \parallel Q) \right|^+ \right\} \tag{8}
\]
\[
= \min_{Q(x)} \min_{U(z), W(y \mid z)} \left\{ D(UW \parallel UP) + D(U \parallel Q) \right\}, \tag{9}
\]
\[
\geq \min_{U(z), W(y \mid z)} \left\{ D(UW \parallel UP), R - I(U, W) + D(UW \parallel UP) \right\}, \tag{10}
\]
where (10) is equivalent to (7) since $|t|^+ = \max \{0, t\}$. So that (7), (8), (9), and (10) are all equal. In [7] the inner minimum of (8) was used as a basis of an iterative procedure to find minimizing solutions of (7). In what follows, we modify the method of Csiszár and Tusnády [9] to show convergence of this minimization procedure.

III. CONVERGENCE OF THE ITERATIVE MINIMIZATION FOR FIXED $(R, \alpha)$

Let us define a short notation for the maximum in (9), which is also the objective function of (8):
\[
F_1(UW, Q) \triangleq D(UW \parallel UP) + D(U \parallel Q), \tag{11}
\]
\[
F_2(UW, R) \triangleq D(UW \parallel UP) - I(U, W) + R, \tag{12}
\]
\[
F(UW, Q, R) \triangleq \max \left\{ F_1(UW, Q), F_2(UW, R) \right\}. \tag{13}
\]
Define notation for the inner minimum in (8)-(9):
\[
E_c(Q, R, \alpha) \triangleq \min_{U(z), W(y \mid z)} \left\{ F(UW, Q, R) \right\}. \tag{14}
\]
The iterative minimization procedure from [7], consisting of two steps in each iteration2, is given by
\[
U_{\ell}W_{\ell} \subset \arg \min_{U(z), W(y \mid z): \mathbb{E}_U[f(U)] \leq \alpha} F(UW, Q, R), \tag{15}
\]
\[
Q_{\ell+1} = U_\ell, \quad \ell = 0, 1, 2, \ldots.
\]
Throughout the paper, we also use notation $U \ll Q$ (i.e., $U$ is absolutely continuous w.r.t. $Q$), meaning that $U(x) = 0$ whenever $Q(x) = 0$. We assume that the initial distribution $Q_0$ in (15) is chosen such that the set $\{ U : \sum_x U(x)f(x) \leq \alpha, U \ll Q_0 \}$ is non-empty, which guarantees $F(U_0W_0, Q_0, R) = E_c(Q_0, R, \alpha) < \infty$. By (11) it is clear that (15) produces a monotonically non-increasing sequence $E_c(Q_\ell, R, \alpha), \ell = 0, 1, 2, \ldots$. Our main result is given by the following theorem, which is an improvement on [7, Theorem 1] and [7, Lemma 6]:

**Theorem 1:** Let $\{ U_\ell W_\ell \}_{\ell = 0}^{+\infty}$ be a sequence of iterative solutions produced by (15). Then
\[
E_c(Q_\ell, R, \alpha) \underset{\ell \to \infty}{\longrightarrow} \min_{Q(x)} E_c(Q, R, \alpha), \tag{16}
\]
where $E_c(Q, R, \alpha)$ is defined in (14).

In order to prove Theorem 1, we use a lemma, which is similar to “the five points property” from [9].

**Lemma 1:** Let $\mathbb{UW}$ be such that $\mathbb{UW} \ll Q_0P$ and $\sum_x \mathbb{U}(x)f(x) \leq \alpha$. If $F_1(U_0W_0, Q_0) > F_2(U_0W_0, R)$, then $\mathbb{U} \ll Q_1$ and
\[
F(U_0W_0, Q_0, R) \leq F(U_0W_0, Q_0, R) \leq F(\mathbb{UW}, \mathbb{U}, R) + D(U \parallel Q_0) - D(\mathbb{U} \parallel Q_1). \tag{17}
\]
If $F_1(U_0W_0, Q_0) < F_2(U_0W_0, R)$, then
\[
F(U_0W_0, Q_0, R) \leq F(\mathbb{UW}, \mathbb{U}, R). \tag{18}
\]

2Note that (15) is not just an alternating minimization procedure w.r.t. $F(UW, Q, R)$, or not the only one possible, in a sense that other choices of $Q_{\ell+1}$ may also minimize $F(U_{\ell}W_{\ell}, Q, R)$. For example, in the absence of the channel input constraint, for any $Q$ it already holds that $F(U_{\ell}W_{\ell}, Q, R) \geq F(\mathbb{U}_{\ell}W_{\ell}, Q_{\ell}, R)$, and, in particular, any $Q_\ell$, such that $D(U_{\ell} \parallel Q) \leq D(\mathbb{U}_{\ell} \parallel Q_{\ell})$, will minimize $F(U_{\ell}W_{\ell}, Q, R)$. 2138

...
If $F_1(U_0W_0, Q_0) = F_2(U_0W_0, R)$, then either (18) holds, or, if (18) does not hold, then necessarily $U \ll Q_1$ and (17) holds.

Proof: Let us define a set of distributions $UW$:

$$S \triangleq \left\{ UW : \sum_x U(x)f(x) \leq \alpha, UW \ll Q_0P \right\}.$$  

Observe that $S$ is a closed convex set. Since $\hat{U}W \in S$, then $S$ is non-empty and by (15) we also have $U_0W_0 \in S$.

If $F_2(U_0W_0, Q_0) > F_2(U_0W_0, R)$, then $F_1(U_0W_0, Q_0) = F_1(U_0W_0, Q_0, R)$ by (13). Observe that the function $F_1(UW, Q_0) = D(UW \parallel Q_0P)$ is convex ($\cup$) in $S$, while the second function in the maximization in (13), $F_2(UW, R) = D(UW \parallel UP) - I(U, W) + R$, is continuous in $S$. By (15), we conclude that $F_2(U_0W_0, Q_0)$ cannot be decreased in the vicinity of $U_0W_0$ inside the convex set $S$, and by convexity of $F_1(UW, Q_0)$ it follows that

$$F_1(U_0W_0, Q_0) = \min_{U(x), W(y|x) : \sum_x U(x)f(x) \leq \alpha} F_1(UW, Q_0).$$

Since by definition we have $F_1(UW, Q_0) = D(UW \parallel Q_0P)$, we can apply the “Pythagorean” theorem for divergence [12] (proved as “the three points property” in [9, Lemma 2]) and write:

$$F(U_0W_0, Q_0, R) + D(\hat{U}W \parallel U_0W_0) \leq D(\hat{U}W \parallel Q_0P).$$  \hspace{1cm} (19)

Since $\hat{U}W \ll Q_0P$, we have $D(\hat{U}W \parallel Q_0P) < +\infty$. Then by (19) it also holds that $D(\hat{U}W \parallel U_0W_0) < +\infty$ with $\hat{U} \ll Q_1$. On the other hand, by (13) and (11) we have

$$F(\hat{U}W, \hat{U}, R) \geq F_1(\hat{U}W, \hat{U}) = D(\hat{U}W \parallel \hat{U}P) = D(\hat{U} \parallel Q_1) \geq D(\hat{U}W \parallel Q_1P) - D(\hat{UW} \parallel U_0W_0).$$  \hspace{1cm} (20)

Combining (19) and (20), we obtain (17).

If $F_1(U_0W_0, Q_0) < F_2(U_0W_0, R)$, then $F_2(U_0W_0, R) = F(U_0W_0, Q_0, R)$ by (13). Now we observe that the first function in the maximization in (13), $F_1(UW, Q_0) = D(UW \parallel Q_0P)$, is continuous in $S$, while the second function $F_2(UW, R) = D(UW \parallel UP) - I(U, W) + R$ is convex ($\cup$) in $S$. By (15), we conclude that $F_2(U_0W_0, R)$ cannot be decreased in the vicinity of $U_0W_0$ inside the convex set $S$, and by convexity of $F_2(UW, R)$ it follows that

$$F_2(U_0W_0, R) = \min_{U(x), W(y|x) \leq \alpha} F_2(UW, R) \leq F_2(\hat{U}W, R) \leq F(\hat{U}W, \hat{U}, R),$$

where (a) follows because $\hat{U}W \in S$, and (b) follows by (13). This gives (18).

Assume now that the last case holds, that is $F_1(U_0W_0, Q_0) = F_2(U_0W_0, R)$. Let us define

$$U^{(\lambda)}(x)W^{(\lambda)}(y|x) \triangleq \lambda\hat{U}(x)\hat{W}(y|x) + (1 - \lambda)U_0(x)W_0(y|x), \ \lambda \in (0, 1).$$  \hspace{1cm} (21)

We have that $U^{(\lambda)}W^{(\lambda)} \in S$, and the two functions $f_1(\lambda) \triangleq F_1(U^{(\lambda)}W^{(\lambda)}, Q_0)$ and $f_2(\lambda) \triangleq F_2(U^{(\lambda)}W^{(\lambda)}, R)$ are convex ($\cup$) and differentiable w.r.t. $\lambda \in (0, 1)$. By (13), (15), at least one of these functions has to be non-decreasing at $\lambda = 0$:

$$\lim_{\lambda \to 0} \frac{df_1(\lambda)}{d\lambda} \geq 0 \ \text{or} \ \lim_{\lambda \to 0} \frac{df_2(\lambda)}{d\lambda} \geq 0.$$  

The first condition results in (19), which guarantees $\hat{U} \ll Q_1$ and (17). The second condition implies

$$F_2(U_0W_0, R) \leq F_2(\hat{U}W, R) \leq F(\hat{U}W, \hat{U}, R),$$

where the second inequality is by definition (13). This gives (18). □

Proof of Theorem 1: By (7)-(10) we can rewrite the RHS of (16) as

$$\min_{Q \ll Q_0} E_c(Q, R, \alpha) = \min_{Q \ll Q_0} E_c(Q, R, \alpha).$$  \hspace{1cm} (22)

Suppose (22) is finite, and let $\hat{U}W$ achieve the minimum in (22). Then $\hat{U}W \ll Q_0P$ and $\sum_x U(x)f(x) \leq \alpha$. Then Lemma 1 implies that there exists only two possibilities for the outcome of the iterations in (15). One possibility is that at some iteration $\ell$ it holds that

$$F(U_\ell W_\ell, Q_\ell, R) \leq F(\hat{U}W, \hat{U}, R),$$

meaning that the monotonically non-increasing sequence of $F(U_\ell W_\ell, Q_\ell, R) = E_c(Q_\ell, R, \alpha)$ has converged to (22). The alternative possibility is that for all iterations $\ell = 0, 1, 2, \ldots$, it holds that

$$F(U_\ell W_\ell, Q_\ell, R) \leq F(\hat{U}W, \hat{U}, R) + D(\hat{U} \parallel Q_\ell) - D(\hat{U} \parallel Q_{\ell+1}),$$

with all terms finite. Now, just like in [9, Lemma 1], it has to be true that

$$\liminf_{\ell \to \infty} \left\{ D(\hat{U} \parallel Q_\ell) - D(\hat{U} \parallel Q_{\ell+1}) \right\} = 0,$$

because the divergence is non-negative (i.e., bounded from below). Therefore $F(U_\ell W_\ell, Q_\ell, R)$ must converge to $F(\hat{U}W, \hat{U}, R)$, yielding (22), and this concludes the proof of Theorem 1. □

IV. CONVERGENCE OF THE ITERATIVE MINIMIZATION FOR FIXED GRADIENT

Let us define for two real numbers $\rho$ and $\eta$

$$F(\rho, \eta, UW, Q) \triangleq D(UW \parallel UP) + (1 - \rho)D(U \parallel Q) - \rho I(U, W) + \eta E_U[f(X)].$$  \hspace{1cm} (23)

$$E_0(\rho, \eta, Q) \triangleq \min_{U(x), W(y|x)} F(\rho, \eta, UW, Q).$$  \hspace{1cm} (24)

The quantity $E_0(\rho, \eta, Q)$ has a meaning of the vertical axis intercept (“$E_0^*$”) of a lower supporting plane in the variables $(R, \alpha)$ for the function $E(R, \alpha) = E_0(Q, R, \alpha)$, defined in (14), as the following lemma shows.

Lemma 2: For any $0 \leq \rho < 1$ and $\eta \geq 0$ it holds that

$$E_c(Q, R, \alpha) \geq E_0(\rho, \eta, Q) + \rho R - \eta \alpha,$$  \hspace{1cm} (25)
and there exist $R \geq 0$ and $\alpha \geq \min_x f(x)$ which satisfy (25) with equality.

Proof: By definition (14)

$$\min_{U(x), W(y \mid x)} \left\{ D(UW \parallel QP) + |R - I(U, W) - D(U \parallel Q)|^+ \right\} \geq \min_{U(x), W(y \mid x)} \left\{ D(UW \parallel QP) + \rho[R - I(U, W) - D(U \parallel Q)] + \eta[\mathbb{E}_U[f(X)] - \alpha] \right\} \geq \min_{U(x), W(y \mid x)} \left\{ D(UW \parallel QP) + \rho[R - I(U, W) - D(U \parallel Q)] + \eta[\mathbb{E}_U[f(X)] - \alpha] \right\},$$

(26)

where (a) holds for any $0 \leq \rho < 1$ and $\eta \geq 0$. Using (23) and (24), we see that the lower bound expression (27) is equal to the RHS of (25). Let $U_{\rho, x}$ denote distributions $U, W, \ldots$ jointly minimize (27). Observe that for each $0 \leq \rho < 1$ and $\eta \geq 0$ we can find $R \geq 0$ and $\alpha \geq \min_x f(x)$, such that the differences in the square brackets are zero. In this case, $U_{\rho, x}$ will satisfy the input constraint and there will be equality between (27) and (26). \ensuremath{\Box}

In fact, since $E_c(Q, R, \alpha)$ is a convex ($\cup$) and monotonic function of $(R, \alpha)$, which cannot have lower supporting planes with slopes $\rho > 1$, the supremum of the RHS of (25) over $0 \leq \rho < 1$ and $\eta \geq 0$ equals $E_c(Q, R, \alpha)$ for all $(R, \alpha)$.

**Lemma 3:** For $0 \leq \rho < 1$ and $\eta \geq 0$, the unique minimizing solution of the minimum (24) is given by

$$U^*(x)W^*(y \mid x) = \frac{1}{K} Q(x)P_\eta^{\downarrow}P_\eta^{-\downarrow}(x, y) \left[ \sum_a Q(a)P_\eta^{\downarrow}P_\eta^{-\downarrow}(a, y) \right]^{-\rho}, \quad (28)$$

where $P_\eta(x, y) \equiv e^{-\eta f(x)}P(y \mid x)$ and $K$ is a normalization constant, resulting in

$$E_0(\rho, \eta, Q) = -\log \sum_y \left[ \sum_x Q(x)P_\eta^{\downarrow}P_\eta^{-\downarrow}(x, y) \right]^{1 - \rho}. \quad (29)$$

**Proof:** Similarly to [7, Lemma 3]. \ensuremath{\Box}

An iterative minimization procedure at a fixed gradient $(\rho, \eta)$ uses the explicit computation of (28) and is given by

$$U_0 W_0 = \arg\min_{U(x), W(y \mid x)} F(\rho, \eta, UW, Q),$$

$$Q_{\ell+1} = \arg\min_{Q(x)} F(\rho, \eta, U_\ell W_\ell, Q) = U_\ell, \quad (30)$$

where the update of $U_\ell W_\ell$ is according to the expression (28) with $Q$ replaced by $Q_\ell$. The main result of the section is given by the following theorem:

**Theorem 2:** Let $\{U_\ell, W_\ell\}_{\ell=0}^{+\infty}$ be a sequence of iterative solutions produced by (30). Then

$$E_0(\rho, \eta, Q_\ell) \xrightarrow{\ell \to \infty} \min_{Q(x)} E_0(\rho, \eta, Q), \quad (31)$$

where $E_0(\rho, \eta, Q)$ is defined in (24).

In order to prove Theorem 2, we use the following lemma:

**Lemma 4:** Let $\hat{W}$ be such that $\hat{W} \ll Q_0 P$. Then $\hat{W} \ll Q_1$ and

$$F(\rho, \eta, U_0 W_0, Q_0) \leq F(\rho, \eta, \hat{W}, \hat{U}) + (1 - \rho)D(\hat{U} \parallel Q_0) - (1 - \rho)D(\hat{U} \parallel Q_1).$$

**Proof:** Let $U^{(X)}W^{(X)}$ be a convex combination of $\hat{W}$ and $U_0 W_0$, as in (21). Then the function $F(\rho, \eta, U^{(X)}W^{(X)}, Q_0) = g(\lambda)$ is convex ($\cup$) and differentiable in $\lambda \in (0, 1)$. Since $U_0 W_0$ achieves the minimum of $F(\rho, \eta, UW, Q_0)$ over $UW$, then necessarily

$$\lim_{\lambda \to 0} \frac{dg(\lambda)}{d\lambda} \geq 0.$$ 

Differentiation results in the following condition in the limit:

$$F(\rho, \eta, \hat{W}, Q_0) \leq F(\rho, \eta, U_0 W_0, Q_0) - (1 - \rho)D(\hat{W} \parallel U_0 W_0) - (1 - \rho)D(\hat{U} \parallel T_0) \geq 0, \quad (33)$$

where $\hat{T}$ and $T_0$ denote the $y$-marginal distributions of $\hat{W}$ and $U_0 W_0$, respectively. It follows that $D(\hat{U}W \parallel U_0 W_0) < +\infty$ and therefore $\hat{W} \ll Q_1$. On the other hand, by (23)

$$F(\rho, \eta, \hat{U}, \hat{W}) = F(\rho, \eta, \hat{W}, Q_0) - (1 - \rho)D(\hat{U} \parallel Q_0).$$

Combining this with (33), omitting $\rho D(\hat{T} \parallel T_0)$ and replacing $D(UW \parallel U_0 W_0)$ with $D(\hat{U} \parallel U_0)$, we obtain a weaker inequality (32). \ensuremath{\Box}

**Proof of Theorem 2:** Using (23), (24), it can be verified, that the RHS of (31) can be rewritten as

$$\min_{Q(x)} E_0(\rho, \eta, Q) = \min_{U(x), W(y \mid x)} F(\rho, \eta, UW, U). \quad (34)$$

Let $\hat{W}$ achieve the minimum in (34). Then by Lemma 4 we conclude that for all iterations $\ell = 0, 1, 2, \ldots$, it holds that

$$F(\rho, \eta, U_\ell W_\ell, Q_\ell) \leq F(\rho, \eta, \hat{W}, \hat{U}) + (1 - \rho)D(\hat{U} \parallel Q_\ell) - (1 - \rho)D(\hat{U} \parallel Q_{\ell+1}).$$

The conclusion of the proof is the same as in Theorem 1. \ensuremath{\Box}

The next two sections show convergence of fixed-slope computation in the directions of $R$ and $\alpha$, respectively. They are similar in structure to Section IV.

**V. CONVERGENCE FOR FIXED $\alpha$ AND $\rho$**

In this section we show convergence of an iterative minimization at a fixed slope $\rho$ in the direction of $R$, i.e., for a given $\alpha$. With the help of (23) let us define $F(\rho, UW, Q) \triangleq F(\rho, \eta, UW, Q)|_{\eta=0}$ and

$$E_0(\rho, Q, \alpha) \triangleq \min_{U(x), W(y \mid x): \mathbb{E}_U[f(X)] \leq \alpha} F(\rho, \eta, UW, Q). \quad (35)$$

2140
Lemma 5: For any 0 ≤ ρ < 1 it holds that
\[ E_0(ρ, Q, α) ≥ E_0(ρ, Q, α) + ρR, \] (36)
and there exists \( R ≥ 0 \) which satisfies (36) with equality.
Proof: Similar to Lemma 2. □

An iterative minimization procedure at a fixed slope \( ρ \) is given by
\[ U_ℓ W_ℓ ∈ \arg \min_{U(x), W(y|x)} F(ρ, U, W, Q), \]
\[ Q_ℓ+1 = \arg \min_{Q(x)} F(ρ, U_ℓ W_ℓ, Q) = U_ℓ, \] (37)
\[ ℓ = 0, 1, 2, \ldots. \]
It is assumed that \( Q_0 \) is chosen such that the set \( \{ U : \sum_x U(x)f(x) ≤ α, U ≪ Q_0 \} \) is non-empty, so that
\[ F(ρ, U_0 W_0, Q_0) = E_0(ρ, Q_0, α) = +∞. \] The main result of this section is stated in the following theorem.

Theorem 3: Let \( \{ U_ℓ W_ℓ \}_{ℓ=0}^{+∞} \) be a sequence of iterative solutions produced by (37). Then
\[ E_0(ρ, Q, α) \xrightarrow{ℓ→∞} \min_{Q(x)} E_0(ρ, Q, α), \] (38)
where \( E_0(ρ, Q, α) \) is defined in (35).
To prove Theorem 3, we use a lemma, similar to Lemma 4:

Lemma 6: Let \( U W \) be such that \( U W ≪ Q_0 P \) and
\[ \sum_x U(x)f(x) ≤ α. \] Then \( U ≪ Q_1 \) and
\[ F(ρ, U_0 W_0, Q_0) ≤ F(ρ, U W, U) \]
\[ + (1 - ρ)D(U || Q_0) - (1 - ρ)D(U || Q_1). \] (39)
Proof: Analogous to Lemma 4. □

Proof of Theorem 3: The RHS of (38) can be rewritten in terms of \( F(ρ, U, W, Q) \) as:
\[ \min_{Q(x) \ll Q_0} E_0(ρ, Q, α) = \min_{U(x), W(y|x)} F(ρ, U, W, U). \] (40)
Suppose (40) is finite and \( U W \) achieves the minimum on the RHS. Then we can use Lemma 6 with \( U W \). The rest of the proof is the same as for Theorem 2. □

VI. CONVERGENCE FOR FIXED \( R \) AND \( η \)

In this section we show convergence of an iterative minimization at a fixed slope \( η \) in the direction of \( α \), i.e., for a given \( R \). Let us define
\[ F(η, U, W, Q, R) \equiv \max \left\{ F_1(U, W, Q), F_2(U, W, R) \right\} + ηE_U[f(X)], \] (41)
where \( F_1(U, W, Q) \) and \( F_2(U, W, R) \) are as defined in (11) and (12), respectively.
\[ E_0(η, Q, R) \equiv \min_{U(x), W(y|x)} F(η, U, W, Q, R). \] (42)
Here \( E_0(η, Q, R) \) plays a role of “\( E_0 \)” of a supporting line in the variable \( α \) of the function \( F(α) = E_0(η, Q, R, α) \), defined in (14), as shown by the following lemma.

Lemma 7: For any \( η ≥ 0 \) it holds that
\[ E_0(η, Q, R, α) ≥ E_0(η, Q, R) - ηα, \] (43)
and there exists \( α ≥ \min x f(x) \) which satisfies (43) with equality.
Proof: Similar to Lemma 2. □

An iterative minimization procedure at a fixed slope \( η \) is defined as follows.
\[ U_ℓ W_ℓ ∈ \arg \min_{U(x), W(y|x)} F(η, U, W, Q, R), \]
\[ Q_ℓ+1 = U_ℓ, \] (44)
\[ ℓ = 0, 1, 2, \ldots. \]
This procedure results in a monotonically non-increasing sequence \( E_0(η, Q_ℓ, R), ℓ = 0, 1, 2, \ldots \), as can be seen from (41), (42). The sequence converges to the global minimum in the support of \( Q_0 \), as stated in the following theorem.

Theorem 4: Let \( \{ U_ℓ W_ℓ \}_{ℓ=0}^{+∞} \) be a sequence of iterative solutions produced by (44). Then
\[ E_0(η, Q, R) \xrightarrow{ℓ→∞} \min_{Q(x) \ll Q_0} E_0(η, Q, R), \] (45)
where \( E_0(η, Q, R) \) is defined in (42).
To prove this theorem, we use a lemma, which is similar to Lemma 1:
Lemma 8: Let \( U W \) be such that \( U W ≪ Q_0 P \).
If \( F_1(U_0 W_0, Q_0) > F_2(U_0 W_0, R) \), then \( U ≪ Q_1 \) and
\[ F(η, U_0 W_0, Q_0, R) ≤ F(η, U W, U) + D(U || Q_0) - D(U || Q_1). \] (46)
If \( F_1(U_0 W_0, Q_0) < F_2(U_0 W_0, R) \), then
\[ F(η, U_0 W_0, Q_0, R) ≤ F(η, U W, U, R). \] (47)
If \( F_1(U_0 W_0, Q_0) = F_2(U_0 W_0, R) \), then either (47) holds, or if (47) does not hold, then necessarily \( U ≪ Q_1 \) and (46) holds.
Proof: Similar to Lemma 1. □

Proof of Theorem 4: The RHS of (45) can be rewritten in terms of \( F(η, U, W, Q, R) \) as:
\[ \min_{Q(x) \ll Q_0} E_0(η, Q, R) = \min_{U(x), W(y|x)} F(η, U, W, U, R). \] (48)
Let \( U W \) achieve the minimum on the RHS. Then we can use Lemma 8 with \( U W \). The rest of the proof is the same as for Theorem 1. □

REFERENCES
[1] G. Dueck and J. Körner, “Reliability Function of a Discrete Memoryless Channel at Rates above Capacity,” IEEE Trans. on Information Theory, vol. 25, no. 1, pp. 82–85, Jan 1979.
[2] S. Arimoto, “Computation of Random Coding Exponent Functions,” IEEE Trans. on Information Theory, vol. 22, no. 6, pp. 665–671, Nov 1976.
[3] S. Arimoto, “On the Converse to the Coding Theorem for Discrete Memoryless Channels,” IEEE Trans. on Information Theory, vol. 19, no. 3, pp. 357–359, May 1973.
[4] Y. Oohama and Y. Jitsumatsu, “A New Iterative Algorithm for Computing the Correct Decoding Probability Exponent of Discrete Memoryless Channels,” IEEE Trans. on Information Theory (Early Access), Oct 2019.

[5] Y. Oohama and Y. Jitsumatsu, “A New Iterative Algorithm for Computing the Optimal Exponent of Correct Decoding for Discrete Memoryless Channels,” in IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, Jun 2015.

[6] R. G. Gallager, “Information Theory and Reliable Communication,” John Wiley & Sons, 1968.

[7] S. Tridenski and R. Zamir, “Channel Input Adaptation via Natural Type Selection,” IEEE Trans. on Information Theory, vol. 66, no. 4, pp. 2078–2090, Apr 2020.

[8] S. Tridenski and R. Zamir, “Exponential Source/Channel Duality,” in IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, Jun 2017.

[9] I. Csiszár and G. Tusnády, “Information Geometry and Alternating Minimization Procedures,” Statistics & Decisions, no. 1, pp. 205–237, 1984.

[10] S. Tridenski, A. Somekh-Baruch, R. Zamir, “Proof of Convergence for Correct-Decoding Exponent Computation,” arXiv, vol. abs/2001.05711, 2020.

[11] Y. Oohama, “Exponent Function for Stationary Memoryless Channels with Input Cost at Rates above the Capacity,” arXiv, vol. abs/1701.06545, 2017.

[12] T. M. Cover and J. A. Thomas, “Elements of Information Theory,” John Wiley & Sons, 1991.