Feedback Halves the Dispersion for Some Two-User Broadcast Channels with Common Message
Trillingsgaard, Kasper Fløe; Yang, Wei; Durisi, Giuseppe; Popovski, Petar

Published in:
2017 IEEE International Symposium on Information Theory (ISIT)

DOI (link to publication from Publisher):
10.1109/ISIT.2017.8006517

Publication date:
2017

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
https://doi.org/10.1109/ISIT.2017.8006517
Feedback Halves the Dispersion for Some Two-User Broadcast Channels with Common Message

Kasper Fløe Trillinggaard\textsuperscript{1}, Wei Yang\textsuperscript{2}, Giuseppe Durisi\textsuperscript{3}, and Petar Popovski\textsuperscript{1}

\textsuperscript{1}Aalborg University, 9220, Aalborg Øst, Denmark
\textsuperscript{2}Princeton University, 08544, Princeton, USA
\textsuperscript{3}Chalmers University of Technology, 41296 Gothenburg, Sweden

Abstract—We investigate the maximum coding rate achievable on a two-user broadcast channel for the case where a common-message is transmitted using fixed-blocklength codes with feedback. Specifically, we focus on a family of broadcast channels composed of two antisymmetric Z-channels. For this setup, we obtain matching upper and lower bounds on the dispersion term in the asymptotic expansion of the maximum coding rate. These bounds reveal that the dispersion is halved compared to the no-feedback case.

I. INTRODUCTION

We consider a two-user common-message discrete-time memoryless broadcast channel (CM-BC) with full feedback. As for the point-to-point setup, it is well known that feedback does not improve capacity, which is given by

\[ C = \sup_{P} \min_{k \in \{1,2\}} I(P, W_k). \]  

(1)

Here, \( W_1 \) and \( W_2 \) denote the component channels from the encoder to the two decoders and the supremum is over all input distributions \( P \).

In this paper, we show that there exist CM-BCs for which feedback improves the speed at which the maximum coding rate achievable with fixed-blocklength codes approaches capacity as the blocklength increases. Specifically, we shall focus (for simplicity) on the class of CM-BCs consisting of two antisymmetric Z-channels \( W_1 \) and \( W_2 \) defined as follows:

\[ W_1(0|0) = 1 - W_1(1|0) = W_2(1|1) = 1 - W_2(0|1) = 1 \]  
\[ W_1(0|1) = 1 - W_1(1|1) = W_2(1|0) = 1 - W_2(0|0) = \delta. \]  

(2)

(3)

Here, \( \delta \in (0,1) \). Note that for this class of CM-BCs, which we shall refer to as AZ-CM-BCs (AZ stands for antisymmetric Z), the capacity-achieving input distribution (CAID) \( P^* \) is the uniform distribution.

For the no-feedback case, a CM-BC is equivalent to a compound channel, whose second-order coding rates (i.e., the second-order expansion of the maximum coding rate in the limit of large blocklength) were investigated in [1]. There, it was proven that the second-order term in the expansion of the logarithm of maximum number of codewords \( M^*(n, \epsilon) \) as a function of the blocklength \( n \) and the average error probability \( \epsilon \in (0,1) \) is in general a function of both the \textit{dispersions} [2, Eq. (222)] of the individual component channels and of the directional derivatives of their mutual informations computed at the CAID. The particular structure of the antisymmetric Z-channel setup considered in this paper yields, however, the following drastic simplification to the second-order expansion of \( \log M^*(n, \epsilon) \) for the no-feedback case:

\[ \log M^*(n, \epsilon) = nC - \sqrt{nV} Q^{-1} (\epsilon) + o(\sqrt{n}). \]  

(4)

Here, \( V \) is the conditional information variance (see [2, Eq. (242)]) evaluated at \( P^* \) which is the same for \( W_1 \) and \( W_2 \).

When \textit{variable-length codes} are used, feedback is known to improve the speed at which the maximum coding rate converges to capacity. Specifically, it was shown in [3] that the square-root term in the asymptotic expansion of the maximum coding rate (cf. (4)) vanishes for point-to-point discrete memoryless channels (DMCs), a result known as zero-dispersion. Furthermore, this fast convergence to capacity can be achieved using only stop feedback (also known as decision feedback). Namely, the feedback channel is used only to stop transmissions. For CM-BCs, however, stop feedback is not sufficient to achieve zero-dispersion. Specifically, we recently showed that the asymptotic expansion of the maximum coding rate with variable-length codes and stop feedback contains a square-root penalty term, provided that some mild technical conditions are satisfied [4].

In the fixed-blocklength-code setup, it is known that feedback does not improve the second-order term for point-to-point DMCs under certain symmetry conditions. Specifically, it was shown in [3] that feedback does not improve the second-order term for weakly input-symmetric DMCs. This result was extended to a broader class of DMCs in [5], where it was shown that the same holds when the conditional information variance is constant for all input symbols.

\textbf{Contributions:} We show that, in the fixed-blocklength-code setup, the availability of feedback yields an improvement to the second-order term of the asymptotic expansion of \( \log M^*(n, \epsilon) \) for CM-BCs composed of two antisymmetric Z-channels. Specifically, we demonstrate that, when \( \epsilon \in (0, 1/2) \), the second-order term in (4) can be improved to \( \sqrt{nV/2} Q^{-1}(2\epsilon) \) if feedback is available, and that this value is optimal.

The intuition behind our result is as follows: feedback allows the encoder to compute the accumulated information density at both decoders and to adapt the input distribution accordingly. Specifically, the encoder makes small adjustments to the input distribution in order to favor the decoder with the smallest information density and to drive both information densities
close to their arithmetic mean. The problem of computing the maximum coding rate then becomes roughly equivalent to the one of computing the \( \epsilon \)-quantile of the arithmetic mean of the two information densities. The desired result follows because the arithmetic mean of the two information densities has variance \( V/2 \). Hence, the dispersion is halved. Furthermore, the improvement from \( Q^{-1}(\epsilon) \) to \( Q^{-1}(2\epsilon) \) is achieved as follows: if the arithmetic mean of the information densities is below a suitably chosen threshold shortly before the end of the transmission, the encoder can change the input distribution to either the CAID of \( W_1 \) or the one of \( W_2 \). In this way, it can ensure that at least one of the two decoders is successful.

Extensions: Our results can be extended to a broader class of CM-BCs. In particular, a feedback scheme similar to the one considered in this paper yields an improved second-order term for all CM-BC for which \( P^* \) is the unique maximizer in (1), it satisfies \( P^*(x) > 0 \) for all inputs \( x \), and it is neither the CAID of \( W_1 \) nor of \( W_2 \). Our converse result requires certain additional symmetry conditions.

II. SYSTEM MODEL

We consider the family of AZ-CM-BCs described in Section I. We also assume that the channel outputs at any given time \( i \) are conditionally independent given the input, namely

\[
P_{Y_1,Y_2|X_i}(y_1,i,y_2,i|x_i) = W_1(y_1,i|x_i)W_2(y_2,i|x_i).
\]

An \((n,M,\epsilon)\)-feedback code for this channel consists of:

1. \( n \) encoding functions \( f_i : \{1,\ldots,M\} \times \{0,1\}^{i-1} \to \{0,1\}^1, i = 1,\ldots,n, \) mapping the message \( J \), drawn uniformly from \( \{1,\ldots,M\} \), and the past channel outputs to the channel input \( X_i = f_i(J,Y_{i-1}^2) \).
2. Two decoders \( g_k : \{0,1\}^n \to \{1,\ldots,M\} \) satisfying

\[
\max_{j \in \{1,\ldots,M\}} P[g_k(Y^*_k) \neq j | J = j] \leq \epsilon, \quad k \in \{1,2\}.
\]

The maximum number of codewords with blocklength \( n \) and maximum error probability not exceeding \( \epsilon \) is denoted by

\[
M^*_n(n,\epsilon) = \max\{M : \exists (n,M,\epsilon)\text{-feedback code}\}.
\]

Let \( PW_k(\cdot) \) and \( P \times W_k(\cdot) \) be the marginal output distribution and the joint probability distribution of \((X,Y_k)\), respectively, induced by the input distribution \( P \). For every input distribution \( P \) and \( n \in \mathbb{N} \), we denote the information density between the vectors \( x^n \) and \( y^n_k \) as

\[
i_{P,W_k}(x^n;y^n_k) = \sum_{i=1}^{n} \log \frac{W_k(y_k|x_i)}{PW_k(y_k,i)}.
\]

We let \( I_k(P) = \mathbb{E}_{P \times W_1}[i_{P,W_1}(X;Y_k)] \) be the mutual information and \( V_k(P) = \mathbb{E}_P[\text{Var}_{W_k}[i_{P,W_k}(X;Y_k)|X]] \) be the conditional information variance. The capacity of the AZ-CM-BC is given in (1) and is achieved by the uniform distribution \( P^* \). We denote by \( C_1 = C_2 = C \) the capacities of the two component channels. Finally, we let \( V = V_1(P^*) = V_2(P^*) \) and \( I_k \)

be the derivative of \( I_k([p,1-p]) \) with respect to \( p \) evaluated at \( p = 1/2 \). The following two properties, which are satisfied for the AZ-CM-BC because of antisymmetry, are crucial for establishing our asymptotic result:

\[
I'_1 + I'_2 = 0
\]

and, for \( x \in \{0,1\} \),

\[
\text{Var} \left[i_{P^*,W_1}(x;Y_1) + i_{P^*,W_2}(x;Y_2) \bigg| X = x \right] = 2V.
\]

III. NONASYMPTOTIC BOUNDS

We first state a Verdù-Han-type converse bound for feedback codes. Its proof (which is omitted) relies on the meta-converse theorem [2, Th. 27] and on the inequality [2, Eq. (106)].

Theorem 1: Every \((n,M,\epsilon)\)-feedback code for the AZ-CM-BC satisfies

\[
\epsilon \geq \max_k \left[ \sum_{i=1}^{n} i_{P^*,W_k}(Y_{k,i};f_i(J,Y_{1}^{i-1},Y_{2}^{i-1})) \right] \leq \log M - \eta - e^{-\eta}, \quad \forall \eta > 0.
\]

Before stating our achievability bound, we need to introduce some notation. Throughout this section, we let \( S \supseteq \{1,\ldots,S\} \) and \( L \supseteq \{1,\ldots,L\} \). Furthermore, we set \( \Delta \triangleq \{0,1\}^{SL} \) and index an element \( x \) of \( \Delta \) as follows

\[
x = (s_1(1),\ldots,s_1(S),\ldots,s_L(1),\ldots,s_L(S)).
\]

Here, \( s_k(s) = (s_{k,1}(s),\ldots,s_{k,m}(s)) \in \{0,1\}^m \). For a given vector \( b^\ell \in S^\ell \), we let \( x(b^\ell) = (s_{1}(b^1),\ldots,s_{L}(b^L)) \). Finally, we let \( e^\epsilon(n_B,S^L) \) denote the minimum error probability achievable on an AZ-CM-BC using fixed-blocklength codes with no feedback of blocklength \( n_B \) and with \( S^L \) codewords.

Next, we state our achievability bound.

Theorem 2: Let \( P_1,\ldots,P_3 \) be types of sequences in \( \{0,1\}^m \), let \( \tau \in (0,\epsilon) \) and \( \zeta > 0 \) be arbitrary, and let \( \{h_\ell\}^L_{\ell=1} \) be arbitrary mappings from \( \{0,1\}^L \times \{0,1\}^{SL} \times \{0,1\}^{\ell_m} \) to \( S \). Then,

\[
\log M^*_n(Lm + n_B,\epsilon + \epsilon^\epsilon(n_B,S^L))
\]

\[
\geq \sup \left\{ \gamma : \min_k \text{Pr}\left[ y_k(x^\ell(B^L);Y_k^L(B^L)) \leq \gamma \right] < \epsilon - \tau - e^{-\zeta} \right\}
\]

\[
+ \log \tau - SL\log(1 + m) - L(1 + m) \log S - \zeta.
\]

Here, \( x \in \Delta \) is an arbitrary element of

\[
\mathbb{F} \triangleq \left\{ x \in \Delta : x_\ell(b) \text{ has type } P_\ell, \quad \forall b \in S, \ell \in L \right\}
\]

and \( \mathbb{P}[\cdot] \) denotes the probability distribution of \((Y_1,Y_2,B^L)\) on \( \mathbb{A} \times \Delta \times S^L \) defined by

\[
\mathbb{P}(y_1,y_2,b^L) \triangleq \left( \prod_{\ell=1}^{L} \prod_{s=1}^{S} \prod_{k} W_k^{n}(y_{k,s}(s)|x_\ell(s)) \right)
\]

\[
\times \prod_{\ell=0}^{L-1} \text{I}\left\{ h_\ell(x_\ell(b^\ell),y_{1}^\ell(b^\ell),y_{2}^\ell(b^\ell)) = b_{\ell+1} \right\}
\]

1Throughout the paper, the index \( k \) belongs always to the set \( \{1,2\} \), although this is sometimes not explicitly mentioned.
for $y_{k,\ell}(b) \in \{0,1\}^m$. Finally, we have defined

$$u_k(x_\ell(b); y_{k,\ell}(b)) \equiv \sum_{i=1}^{m} t_{p_k, \mathcal{W}_k}(x_\ell, i) y_{k,\ell, i}(b)$$

(16)

and

$$u_k(x^L(b^L); y^L_k(b^L)) \equiv \sum_{\ell=1}^{L} u_k(x_\ell(b); y_{k,\ell}(b)).$$

(17)

Sketch of the proof: Each codeword of length $Lm$ is divided into $L$ blocks of length $m$. Within each block $\ell$, feedback is used to compute the index $b_\ell$, which selects one out of the $S$ available subcodewords (the vectors $x_\ell(b)$, $b_\ell = 1, \ldots, S$). We then communicate the sequence $b^L$ to the decoders using a code with $S^L$ codewords of length $nB$. The desired bound then follows by applying the achievability bound [1, Th. 3] for compound DMCs without feedback.

IV. ASYMPTOTIC ANALYSIS

By analyzing Theorem 1 and Theorem 2 in the large-blocklength limit, we obtain the following asymptotic expansion for $\log M^*_\epsilon(n, \epsilon)$.

**Theorem 3:** For every $\epsilon \in (0,1/2)$, we have

$$\log M^*_\epsilon(n, \epsilon) = nC - \sqrt{\frac{nV}{2}} Q^{-1}(2\epsilon) + O(n^{1/3} \log n).$$

(18)

**Remark 1:** The assumption $\epsilon \in (0,1/2)$ is crucial for (18) to hold. Indeed, when $c > 1/2$, one can achieve $\log M^*_\epsilon(n, \epsilon) = nC + o(n)$ by using a standard point-to-point fixed blocklength code of rate $C$ and input distribution $P^*_1$ (the CAID of $W_1$) with probability $1/2$ and another code of rate $C'$ but input distribution $P^*_2$ (the CAID of $W_2$) with probability $1/2$. This implies that the strong converse does not hold.

**Remark 2:** If the error probability constraint (6) is replaced with $P[(g_1(Y_1^n), g_2(Y_2^n)) \neq (J, J)] \leq \epsilon$, then the asymptotic expansion in (18) continues to hold except that $Q^{-1}(2\epsilon)$ is replaced with $Q^{-1}(\epsilon)$.

A. **Proof of Theorem 3: Converse**

Let

$$A_k(j, y_1^n, y_2^n) \equiv \sum_{i=1}^{n} t_{p_k, \mathcal{W}_k}(f_i(j, y_1^{i-1}, y_2^{i-1}); y_{k,i})$$

(19)

and

$$A(j, y_1^n, y_2^n) \equiv \frac{1}{2} \left( A_1(j, y_1^n, y_2^n) + A_2(j, y_1^n, y_2^n) \right).$$

(20)

By Theorem 1, every $(n, M, \epsilon)$-feedback code satisfies

$$\epsilon + e^{-\eta} \geq \max_k P[A_k(j, y_1^n, y_2^n) \leq \log M - \eta] \quad \geq \frac{1}{2} \sum_k P[A_k(j, y_1^n, y_2^n) \leq \log M - \eta] \quad \geq \frac{1}{2} \sum_k P \left[ \bigcup_{i} A_k(j, y_1^n, y_2^n) \leq \log M - \eta \right] \quad \geq \frac{1}{2} P[A(j, Y_1^n, Y_2^n) \leq \log M - \eta].$$

(21)

(22)

(23)

(24)

We observe now that, by symmetry, the probability distribution of $t_{p_1, \mathcal{W}_1}(x; Y_1) + t_{p_2, \mathcal{W}_2}(x; Y_2)$ does not depend on $x \in \{0,1\}$. This implies that the probability distribution of $A(j, Y_1^n, Y_2^n)$ does not depend on $j$ and coincides with the one of a sum of bounded i.i.d. random variables (RVs) with mean $C$ and variance $V/2$ (see (10)). Thus, by the Berry–Esseen central limit theorem [6, Th. V.4], we conclude that

$$P[A(J, Y_1^n, Y_2^n) \leq \log M - \eta] \geq Q \left( \frac{nC - \log M + \eta}{\sqrt{nV/2}} \right) - \frac{c}{\sqrt{n}},$$

(25)

Here, $c$ denotes a nonnegative constant, which depends only on the channel families $\{W_k\}$. We obtain the desired result by substituting (25) in (24), by solving for $\log M$, by setting $\eta = \log n$, and by performing a Taylor expansion of $Q^{-1}(\cdot)$ around $2\epsilon$.

B. **Proof of Theorem 3: Achievability**

To establish the achievability part, we start by setting in Theorem 2 the parameter $S$ (which controls the number of subcodewords available per block) to 5. Let $C^* \equiv [C - \log 5] + 1$ and set the number of blocks and the number of channel uses per block in Theorem 2 to

$$L = L_n \equiv \lfloor n^{1/3} \rfloor \quad \text{and} \quad m = m_n \equiv \lfloor n/L_n \rfloor - k.$$

(26)

We use the remaining $\kappa n$ channel uses to communicate the sequence $B^{L_n} \in \{1, \ldots, 5\}^{L_n}$ to the decoders. Since $\kappa > C^* - \log 5$, the rate of the code, $\log 5/\kappa$, is smaller than $C$. Hence, its error probability can be made to decay exponentially in $L_n$.

$$e^{*}(\kappa L_n, 5^{L_n}) \leq \exp(-\omega L_n)$$

(27)

for some positive constant $\omega$.

Next, we specify the types $\{P_{b}^1\}_{b=1}^{5}$. Let $\rho > 0$ (a constant we shall specify later) and define the following 5 sequences:

$$p_{1, n} \equiv \frac{1}{2} + \frac{\rho n^{-1/3}}{I_1}, \quad p_{2, n} \equiv \frac{1}{2} + \frac{\rho n^{-1/3}}{I_2}.$$

(28)

$$p_{3, n} \equiv 1/2, \quad p_{4, n} \equiv p_{1}^*, \quad \text{and} \quad p_{5, n} \equiv p_{2}^*.$$

Here, $p_{1}^*$ and $p_{2}^*$ parameterize the CAIDs of $W_1$ and $W_2$, respectively. Note that $p_{1, n}$ and $p_{2, n}$ are in the interval $(0,1)$ for sufficiently large $n$. We now let $\mathcal{P}_{b, n} (b \in \{1,3,4,5\})$ be the element of the set $\{i/m_n : i \in \{0, \ldots, m_n\}\}$ that minimizes $|\mathcal{P}_{b, n} - p_{b, 1}|$. Furthermore, we set $p_{b, 2} = 1 - p_{b, 1}$. We then choose the types in Theorem 2 as $P_b = \mathcal{P}_{b, n} \equiv \mathcal{P}_{b, n} - p_{b, n}$. Some observations are in order. Let $P_{b, n} = p_{b, n} - p_{b, n}$; then $\mathcal{P}_{b, n} - \mathcal{P}_{b, n} = O(1/n)$. Hence, since $I_k(\cdot)$ is differentiable,

$$I_k(\mathcal{P}_{b, n}) = I_k(p_{b, n}) + O(1/n), \quad b \in \{1, \ldots, 5\}.$$
The mappings \( \{ h_{\ell} \}_{\ell=0}^{L_n-1} \) which use the feedback to determine which subcodeword to transmit in each block, are chosen as follows: in the first \( L_n - 1 \) blocks, we let the transmitter choose between subcodewords of type \( P_{1,n} \) and of type \( P_{2,n} \) depending on which decoder has the largest accumulated information density. This balances the information densities at the two decoders and makes the difference tightly concentrated around zero (as we shall see later). In the last block, the transmitter chooses a subcodeword of type \( P_{3,n} \) (which approximates the CAID \( P^* \)) if the arithmetic average of the information densities is above a suitably chosen threshold \( \gamma_1 \), specified later in (45). Otherwise it chooses randomly between the subcodeword of type \( P_{4,n} \) (which approximates the CAID of \( W_1 \)) and the one of type \( P_{5,n} \) (which approximates the CAID of \( W_2 \)).

Specifically, we choose the mappings \( \{ h_{\ell} \}_{\ell=0}^{L_n-1} \) as follows: \( h_0 = 2 \) and for \( \ell = 1, \ldots, L_n - 2 \),

\[
\begin{align*}
& h_t(x(B^\ell), Y_1(B^\ell), Y_2(B^\ell)) = 1 + 1 \left\{ t_1(x(B^\ell); Y_1(B^\ell)) \geq t_2(x(B^\ell); Y_2(B^\ell)) \right\}.
\end{align*}
\]

(31)

For \( \ell = L_n - 1 \), let \( T \) be a uniformly distributed RV on \( \{ 1, 2 \} \) and set

\[
\begin{align*}
& h_\ell(x(B^\ell), Y_1(B^\ell), Y_2(B^\ell)) = \begin{cases} 
3, & \text{if } t_1(x(B^\ell); Y_1(B^\ell)) + t_2(x(B^\ell); Y_2(B^\ell)) \geq 2\gamma_1 \\
4, & \text{if } t_1(x(B^\ell); Y_1(B^\ell)) + t_2(x(B^\ell); Y_2(B^\ell)) < 2\gamma_1 \\
5, & \text{if } t_1(x(B^\ell); Y_1(B^\ell)) + t_2(x(B^\ell); Y_2(B^\ell)) < 2\gamma_1 \\
\end{cases}
\end{align*}
\]

(32)

Roughly speaking, the threshold \( \gamma_1 \) is chosen so that \( P_{3,n}, P_{4,n}, \) and \( P_{5,n} \) are used with probability \( (1 - 2\epsilon) \), \( \epsilon \), and \( \epsilon \), respectively. Using Theorem 2 with the parameters listed above, we obtain

\[
\begin{align*}
\log M_t^\ell(n, \epsilon) \geq & \log M_t^\ell(L_{n,m} + \kappa L_n, \epsilon) \\
\geq & \sup \left\{ \gamma : \min P \left[ \mu_k(x(B^{\ell+n}); Y_k(B^{\ell+n})) < \gamma \right] \leq \epsilon - c_1 n^{-1/2} + O(n^{1/3} \log n) \right\}.
\end{align*}
\]

(33)

for some \( c_1 > 0 \). In the last step, we used that \( (\epsilon^* (\kappa L_n, \delta L_n) + \sqrt{n} + e^{-n^{1/3}}) \leq (e^{-\omega L_n} + \sqrt{n} + e^{-n^{1/3}}) \leq c_1 n^{-1/2} \) for sufficiently large \( n \). Now set

\[
\gamma \triangleq \frac{L_{n,m} C - \sqrt{(L_n - 1) m_n V/2}}{Q - 1(2 \epsilon - 2\sqrt{2}(c_1 + c_2)n^{-1/2})}.
\]

(34)

The constant \( c_2 > 0 \) will be defined shortly. The final step of the proof is to show that the following upper bound holds for sufficiently large \( n \)

\[
P [ \mu_k(x(B^{\ell+n}); Y_k(B^{\ell+n})) < \gamma ] \leq \epsilon - c_1 n^{-1/2}.
\]

(35)

The desired result (18) then follows by using (34) and (35) in (33), by observing that \((L_n - 1)m_n = n + O(n^{2/3})\) and by performing a Taylor expansion of \( Q^{-1}(\cdot) \) in (34) around \( 2\epsilon \).

**Proof of (35):** To simplify the notation, we set

\[
Z_{k,\ell,i}^{(b)} \triangleq \tau_{b,\ell,i}(x; Y_k(B))
\]

\[
Z_{k,\ell_1,\ell_2} \triangleq \sum_{\ell = \ell_1}^{\ell_2} Z_{k,\ell,i}^{(b)}.
\]

(36)

\[
Z_{k,\ell_1,\ell_2} \triangleq \sum_{\ell = \ell_1}^{\ell_2} \sum_{i=1}^{m_n} Z_{k,\ell,i}^{(b)}.
\]

(37)

The RVs \( Z_{k,\ell,i}^{(b)} \) are independent for all \( k, b, \ell, \) and \( i \). Note also that \( Z_{k,1,1} = \mu_k(B^{2n}); Y_k(B^{2n}) \). Hence, the left-hand side of (35) can be rewritten as \( P [ Z_{k,1,1} < \gamma ] \).

It will turn out convenient to define the following quantities as well:

\[
Z^{*} \triangleq \frac{1}{2} \sum_{i=1}^{L_n-1} \sum_{k \in \{ 1, 2 \}} \log P_{B_i,n}(x; Y_k(B_i))
\]

\[
A \triangleq \frac{1}{2} \sum_{i=1}^{L_n-1} \sum_{k \in \{ 1, 2 \}} \sum_{l \in \{ 1, 2 \}} \log P_{B_i,n}(x; Y_k(B_i))
\]

\[
E \triangleq \frac{1}{2} (L_{1,1,n} - L_{2,1,n} - 1).
\]

(38)

(39)

(40)

In the remainder of the proof, we shall make use of the following decomposition:

\[
Z_{k,1,1} = Z^* - A - (-1)^k E.
\]

(41)

We next show that \( Z^* \) is accurately approximated by a normal distribution with mean \(( L_{n-1} - 1)m_n C \) and variance \( (L_{n-1} - 1)m_n V/2 \), whereas both \( A \) and \( E \) are of order \( n^{1/3} \). To prove these claims, we rely on the Berry-Esseen central limit theorem, on Höeffding inequality [7], and on the following stabilization lemma, whose proof (omitted) is by mathematical induction.

**Lemma 4 (stabilization lemma):** Let \( \{ X^{(1)}_\ell \} \) and \( \{ X^{(2)}_\ell \} \) be i.i.d. RVs with mean \( \mu_1 > \mu_2 \) satisfying

\[
P [ X^{(b)}_\ell \geq v ] \leq e^{-\beta [ v - \mu_b v ]^2}, \quad P [ X^{(b)}_\ell \leq v ] \leq e^{-\beta [ v - \mu_b v ]^2}
\]

(42)

for all \( b \in \{ 1, 2 \}, \ell \in \mathbb{N}, \) and some \( \beta > 0 \). Here, \( | \cdot |_+ \triangleq \max \{ 0, \cdot \} \). Define the sequence \( \{ Y_\ell \} \) as follows: \( Y_0 = 0 \) and

\[
Y_\ell = \begin{cases} 
Y_{\ell-1} + X^{(1)}_\ell & \text{for } Y_{\ell-1} < 0 \\
Y_{\ell-1} + X^{(2)}_\ell & \text{for } Y_{\ell-1} \geq 0.
\end{cases}
\]

(43)

Let \( c \geq 1 \) satisfy \( \min \{ \mu_1, -\mu_2 \} \geq \sqrt{\pi / \beta} \exp (c^2 / 4) \). Then

\[
P [ | Y_\ell | \geq v ] \leq 2e^{-c \sqrt{v - \mu_1^2 + \mu_2^2}}.
\]

(44)

Let now \( c^2 > 0 \) be arbitrary and define the thresholds

\[
\gamma_1 \triangleq \gamma - m_n C + n^{1/3} \log n
\]

\[
\gamma_2 \triangleq (L_{n-1} - 1)m_n C - c_4 \sqrt{n} \log n.
\]

(45)

(46)

Here, \( \gamma \) was defined in (34). Intuitively, \( \gamma_1 \) is chosen so as to be the \( 2\epsilon \)-quantile of \( Z^* \) for large \( n \), whereas \( \gamma_2 \) is needed to upper-bound the probability of the (rare) event that \( Z^* \) is far smaller than its mean. Note also that \( \gamma_1 > \gamma_2 \) for sufficiently large \( n \). Define the four disjoint events

\[
E_{1,m} \triangleq \left\{ Z^* - A \in [\gamma_2, \gamma_1), T = m \right\}, \quad m \in \{ 1, 2 \}
\]

\[
E_2 \triangleq \left\{ Z^* - A \geq \gamma_1 \right\}, \quad E_3 \triangleq \left\{ Z^* - A < \gamma_2 \right\}.
\]

(47)

(48)
Let $\hat{k} = 1$ when $k = 2$ and $\hat{k} = 2$ when $k = 1$. Using the events defined above, we readily obtain the following upper bound

$$
P[Z_{k,1,L_n} < \gamma] \leq P[\xi_1,k] + P[\xi_2,k \cap \{Z_{k,1,L_n} < \gamma\}] + P[\xi_3]. \tag{49}
$$

In the following, we upper-bounds each of these four probabilities. It turns out that only $P[\xi_1,k]$ yields a nonvanishing contribution.

**Bound on $P[\xi_1,k]$**: We first establish a bound on the tail probability of $A_{n}$ in (47). Since $P_{1,n} = 1 - P_{2,n}$, we can find a sequence $\{\zeta_n\}$ such that

$$
I_1(P_{b,n}) + I_2(P_{b,n}) = 2(C - \zeta_n^{-2/3}), \quad b \in \{1, 2\}. \tag{50}
$$

It follows from the concavity of mutual information, from (28)–(29), from Taylor’s theorem, and from (9) that the sequence $\zeta_n$ is positive and convergent. Since $D(W_1(\cdot|x)||P_{1,n}^*) + D(W_2(\cdot|x)||P_{2,n}^*) = 2C$ for every $x \in \{0, 1\}$, we must also have that

$$
D(P_{b,n}W_1||P_{1,n}^*) + D(P_{b,n}W_2||P_{2,n}^*) = 2\zeta_n^{-2/3} \tag{51}
$$

for all $b \in \{1, 2\}$. Since $\|P_{b,n} - P_{1,n}^*\|_1 = O(n^{-1/3})$, there exists a constant $c_3 > 0$ such that $\sum_{k=1}^n \log P_{b,n}W_k(y)/P_{1,n}^*(y) \leq c_3 n^{-1/3}$ for sufficiently large $n$. Hence, for sufficiently large $n$, we have

$$
P[A \geq n^{1/3}\log n] \leq \exp(-c_3 n^{1/3}\log^2 n) = O(1/n). \tag{52}
$$

Here, we have used (30), that $P_{2,n} = 1 - P_{1,n}$. Hoeffding’s inequality, and that $\zeta_n$ is convergent.

We next upper-bound $P[\xi_1,k]$ as follows:

$$
P[\xi_1,k] \leq \frac{1}{2} P[Z^* < \gamma + n^{1/3}\log n] + O(1/n) \tag{53}
$$

$$
\leq \frac{1}{2} Q\left(\frac{(L_n - 1)m_nC - \gamma_1 - n^{-1/3}\log n}{\sqrt{V(L_n - 1)m_n^2/2}} + \frac{\sqrt{2}c_2}{n^{1/2}}\right) \leq \epsilon / \sqrt{2c_1/n}. \tag{55}
$$

Here, (53) follows from (47) and (52), and because $T$ is equiprobable on $\{1, 2\}$ and independent of $(Y_1, Y_2)$; (54), which holds for some constant $c_2 > 0$ and sufficiently large $n$, follows from the Berry-Esseen central limit theorem [6, Th. V.4]; finally, (55) follows from (34) and (45).

**Bound on $P[\xi_2 \cap \{Z_{k,1,L_n} < \gamma\}]$**: We show that $E$ in (41) is sufficiently positive around 0. To do this, let

$$
F_b^{(b)}(z) \triangleq \frac{1}{2} \sum_{i=1}^{m_n} (Z_{1,1,i}^{(b)} - Z_{2,1,i}^{(b)}) \tag{56}
$$

for $b \in \{1, 2\}$. The $F_b^{(b)}$ are independent RVs. Furthermore, observe that $E = \sum_{b=1}^k F_b^{(b)}$. Since $P_{1,n} = 1 - P_{2,n}$, there must exist a convergent sequence $\{\xi_n\}$ such that

$$
I_1(P_{b,n}) - I_2(P_{b,n}) = -2(-1)^b \rho m_n^{-1/3} + \xi_n^{-2/3}. \tag{57}
$$

Consequently, since $[x_{1,b}(b)]_{m_n}$ is of constant composition, it follows that $E[F_b^{(b)}] = -(-1)^b \rho m_n^{-1/3} + \xi_n^{-2/3} = O(n^{1/3})$ (recall that $\rho > 0$ is a constant that we have not chosen yet). Since $F_b^{(b)}$ can be written as a sum of independent random variables, we conclude, by applying Hoeffding inequality, that

$$
P[F_b^{(b)} \geq \nu] \leq e^{-\frac{2}{\rho n^2} \nu^2} \tag{58}
$$

and

$$
P[F_b^{(b)} \leq \nu] \leq e^{-\frac{2}{\rho n^2} \nu^2}. \tag{59}
$$

Here, $c_5 \geq \max\{1, |Z_{1,1,2} - Z_{2,2,1}|\}$. We now choose $\rho$ so that $\rho > 4\pi^2c_5^2$. Next, we apply Lemma 4 with $X^{(b)} = F_b^{(b)}$, $\beta = 1/(2m_n^c_3)$ and $c = 2c_2$ and obtain

$$
P[|E| \geq n^{1/3}\log n] \leq 2e^{-\frac{2}{\rho n^2} \nu^2(n^{1/3}\log n - 2m_n) \leq 3/n}. \tag{60}
$$

In the last step, which holds for sufficiently large $n$, we used that $\xi_n^{-2/3} = O(1)$. Consider now

$$
P[\xi_2 \cap \{Z_{k,1,L_n} < \gamma\}] \leq P[\xi_2 \cap \{E \leq n^{1/3}\log n, Z_{k,1,L_n} < \gamma\}] + 3/n \tag{61}
$$

$$
\leq P[Z_{k,1,L_n} < \gamma - \gamma_2 + n^{1/3}\log n|B_{L_n} = 3 + k] + 3/n \tag{62}
$$

where $c_6 > 0$ is some constant. Here, (61) follows from (60); (62) follows because if $F_1(k)$ occurs then $B_{L_n} = 3 + k$ (see (32)), because $Z^* - A \geq \gamma_2$, and because $Z_{k,1,L_n} = Z^* - A - (-1)^k E + Z_{k,1,L_n}$. Finally, (63) follows from (34), (46), and Hoeffding inequality applied to $Z_{k,1,L_n}$.

**Bound on $P[\xi_3]$**: We show that $P[\xi_3 \cap \{Z_{k,1,L_n} < \gamma\}] = O(1/n)$ using an argument similar to the one leading to (64) and that $P[\xi_3] = O(1/n)$ using (46), (52), and Hoeffding inequality applied to $Z^*$. Substituting these last two results as well as (55) and (64) into (49), we establish the desired upper bound (55).

**V. Acknowledgements**

The work of K. F. Trillingsgaard and P. Popovski was supported in part by the European Research Council (ERC Consolidator Grant Nr. 648382 WILLOW) within the Horizon 2020 Program. The work of G. Durisi was supported by the Swedish Research Council under the grant 2016-03293.

**References**


