Sphere-packing Bound for Block-codes with Feedback and Finite Memory

Giacomo Como
Massachusetts Institute of Technology
Laboratory for Information and Decision Systems

Barış Nakiboğlu
Massachusetts Institute of Technology
Research Laboratory of Electronics at MIT

Abstract—A lower bound on the error probability of fixed-length block-coding systems with finite memory feedback, which can be described in terms of a time dependent finite state machine. It is shown that the reliability function of such coding systems over discrete memoryless channels is upper-bounded by the sphere-packing exponent.

I. INTRODUCTION

Despite being provably effective in reducing latency as well as complexity of coding systems, and in improving the capacity of certain channels with memory, feedback has been the object of a long history of negative results when it comes to transmission over discrete memoryless channels (DMCs). After Shannon proved that feedback cannot increase the capacity on symmetric DMCs [2], whether such a result continues to hold for non-symmetric DMCs is a long-standing conjecture. An upper bound on the reliability function is given by the Haroutunian exponent [3], which is typically larger than the sphere-packing exponent on non-symmetric DMCs. In [7], the aforementioned conjecture was claimed to be proved, but the proposed proof appears to suffer from major gaps.

In the present paper, we shall be concerned with fixed-length block-coding over DMCs with finite memory feedback. In particular, we shall consider the case when the feedback information can only be stored by a, possibly time-inhomogeneous, finite-state machine, whose state is updated each time a channel output is fed back to the transmitter. Under some mild technical assumptions, we shall prove that the reliability function is upper-bounded by the sphere-packing exponent of the channel.

The proof presented in this paper partially follows the line of reasoning of [7], complementing the two major gaps therein with measure concentration, mixing, and fixed-composition arguments, whose applicability relies on the finite memory assumption. Our results may be thought as complementary to those in [4], where a lower bound on the error probability of block-coding schemes with delayed feedback has been derived.

The remainder of this paper is organized as follows. In Sect. II we describe the transmission model, with the finite memory restriction on the feedback encoders, and state our main result as Theorem 1. Then, in Sect. III we derive a lower bound to the error probability via a change of measure argument, using Holder’s inequality, and give a brief discussion on how the sphere-packing bound can be established when there is no feedback. In Sect. IV, we study the mixing properties of certain Markov chains in order to make a similar measure change argument for the encoding schemes satisfying our assumption. In Sect. V we combine the results of section III and IV using a method of type arguments, and complete the proof of Theorem 1.
Notice that, if one allows for infinite state space $\mathcal{S}$, then any feedback encoder as in (2) can be easily represented in the form (4). In contrast, assuming—as we shall— that (4) holds for some finite $\mathcal{S}$ induces a real constraint. We shall also assume that there exists some $k \geq 1$ such that
\[ \forall t \geq 1, \forall i, j \in \mathcal{S}, \exists y_{t+1}^j \in \mathcal{Y}^k : \Gamma_{t+1}^j(i, y_{t+1}^j) = j. \quad (5) \]
The condition above ensures that effect of past channel outputs whaters away fast enough. Observe, that (4) and (5) are naturally satisfied when $\phi_0(m, y_{t-1}^j) = \phi_0(m, y_{t-2}^j)$, i.e. when the transmitter uses only the latest $k$ channel outputs. Indeed, it is sufficient to choose $\mathcal{S} = \mathcal{Y}^k$ and $\Gamma_1(y_{t-1}^j, y_t) = y_{t+k-1}^j$. We use this fact to establish the following bound on the error probability of finite memory feedback transmission systems.

**Theorem 1:** For any rate $R$, length $n$ blockcode with feedback of the form (4), satisfying (5) on a DMC satisfying (1)
\[ P_e \geq e^{-n (E_{p}(R - e(\epsilon)) + \epsilon(\epsilon))} \quad \forall \epsilon = 1, 2, \ldots, n \quad (6) \]

III. A FIRST LOWER BOUND ON THE ERROR PROBABILITY

Let $V(\cdot | \cdot)$ be the transition probabilities of a DMC with input alphabet $X$, and output alphabet $Y$. Let $Q(\cdot)$ be a probability distribution over $Y$, such that $V(\cdot | x)$ is absolutely continuous with respect to both $W(\cdot | x)$ and $Q(\cdot)$, for all $x \in X$.

For $A \subseteq \mathcal{M}$, define the sets $A_\epsilon$ and $A_{\epsilon}^{-1}$ as
\[ A_\epsilon := \{(m, y^n) : m \in A : \Psi(y^n) \neq m\} \]
\[ A_{\epsilon}^{-1} := \{(m, y^n) : m \in A : \Psi(y^n) = m\} \]

Let the probability distributions $q(\cdot)$ and $v(\cdot)$ over $\mathcal{M} \times \mathcal{Y}^n$ be
\[ q(m, y^n) = \frac{1}{|A|} \prod_{1 \leq t \leq n} Q(y_t) \quad (7a) \]
\[ v(m, y^n) = \frac{1}{|A|} \prod_{1 \leq t \leq n} V(y_t) \phi(m, y_{t-1}^t) \quad (7b) \]

Let $E_c[\cdot]$ be the expectation under $v(\cdot)$. The following result holds for feedback encoders not necessarily satisfying (4).

**Lemma 1:** For all $\beta > 0$, and $A \subseteq \mathcal{M}$,
\[ w(A) \geq v(A_\epsilon) \frac{\beta}{|A|} \sum_{\mathcal{M}} E_{c} \left[ \prod_{t=1}^{n} e^{\beta (\ln \frac{\phi(m, y_{t-1}^t)}{\phi(m, y_{t-2}^t)}) - R} \right]^{-1/\beta} \quad (8a) \]
\[ v(A) \geq 1 - \left[ \frac{|A|}{|A| - 1} \right]^{\frac{1}{1+\beta}} E_{c} \left[ \prod_{t=1}^{n} e^{\beta (\ln \frac{\phi(m, y_{t-1}^t)}{\phi(m, y_{t-2}^t)}) - R} \right]^{1/(1+\beta)} \quad (8b) \]

**Proof:** Using $w(\cdot)$ and $v(\cdot)$ given in (3), (7), and the reverse Holder’s inequality, one gets
\[ E_{c} \left[ \mathbb{1}_{A}(m) e^{\beta (\ln \frac{\phi(m, y_{n-1}^t)}{\phi(m, y_{t-1}^t)})} \right] = \frac{|A|}{|A| - 1} \sum_{\mathcal{M}} \mathbb{1}_{A}(m) v(m, y_{t-1}^t) w(m, y_{t-2}^t) \quad (9) \]
\[ \geq \frac{|A|}{|A| - 1} \sum_{\mathcal{M}} \mathbb{1}_{A}(m, y^n) v(m, y_{t-1}^t) w(m, y_{t-2}^t) \quad (10) \]
\[ \geq \frac{|A|}{|A| - 1} \sum_{\mathcal{M}} \mathbb{1}_{A}(m, y^n) v(m, y_{t-1}^t) w(m, y_{t-2}^t) \quad (11) \]
\[ = \frac{|A|}{|A| - 1} v(A_\epsilon) w(A_{\epsilon})^{-\beta} \quad (12) \]

Following similar steps one can prove that
\[ E_{c} \left[ \mathbb{1}_{A}(m, y^n) e^{\beta (\ln \frac{\phi(m, y_{n-1}^t)}{\phi(m, y_{t-1}^t)})} \right] \geq v(A_\epsilon)^{\beta} w(A_{\epsilon})^{-\beta} \quad (13) \]

Then the lemma follows equations (9), (10) and the observations $q(A_\epsilon) \leq |A|^{-1}$ and $v(A_\epsilon) = 1 - v(A_{\epsilon})$. Note that equations (8a) and (8b) bound the error probability from below. We shall show in the following sections how Lemma 1 leads to Theorem 1. In order to introduce some of the ideas of that proof let us show how Lemma 1 can be used to establish a lower bound on the error probability in the case without feedback.

**Theorem 2:** The error probability of any length-$n$ block code is lower bounded as
\[ P_e \geq e^{-n (E_{p}(R - e(\epsilon)) + \epsilon(\epsilon))} \quad (14) \]

**Proof:** Let $Q(\cdot) = Q_{\rho}(\cdot)$ be in a parametric form to be specified later. Let $V$ for $v(\cdot)$ be
\[ V_{\rho}(y|x) = \frac{W_{\rho}(y|x)Q_{\rho}(y)}{r_{\rho}(x)} \quad (15) \]

where $r_{\rho}(x) = \sum_{y} W_{\rho}(y|x)Q_{\rho}(y)$. Given $m$, the $y_i$’s are mutually independent. Thus,
\[ E_{c} \left[ \prod_{t=1}^{n} e^{\beta (\ln \frac{\phi(m, y_{t-1}^t)}{\phi(m, y_{t-2}^t)}) - R} \right] \quad (16a) \]
\[ v(A) \geq 1 - \frac{1}{|A| - 1} \sum_{\mathcal{M}} \mathbb{1}_{A}(m, y^n) v(m, y_{t-1}^t) w(m, y_{t-2}^t) \quad (16b) \]

3|\epsilon| E_{c}[\epsilon] = \frac{1}{|A| - 1} E_{c}[\epsilon] \quad (17) \]

Thus if $\beta < - \ln \min \{\beta_1, \beta_2\}$ for all $m$ and $t$, the bound $4$
\[ E_{c} \left[ \ln \frac{v(m, y^n)}{\phi(m, y^n)} \right] - E_{c} \left[ \ln \frac{v(m, y^n)}{\phi(m, y^n)} \right] \leq \frac{1}{|A| - 1} \sum_{\mathcal{M}} |\epsilon| E_{c}[\epsilon] \quad (18) \]
implies that
\[ E_{c} \left[ e^{\beta \ln \phi(m, y^n)} \right] \leq e^{\beta D(V_{\rho}[W|x_t(m)]) + \beta^{2} \ln \frac{1}{|A| - 1} + \frac{1}{|A| - 1} \sum_{\mathcal{M}} |\epsilon| E_{c}[\epsilon] \quad (19a) \]
\[ E_{c} \left[ e^{\beta \ln \phi(m, y^n)} \right] \leq e^{\beta D(V_{\rho}[Q_{\rho}|x_t(m)]) + \beta^{2} \ln \frac{1}{|A| - 1} + \frac{1}{|A| - 1} \sum_{\mathcal{M}} |\epsilon| E_{c}[\epsilon] \quad (19b) \]

where $x_t(m)$ is the input letter for message $m$ at time $t$.

For any block-length $n$ there are $\binom{n+1}{k} \leq (n+1)^k$ empirical types. Thus if we choose the messages of the most populous type, say $P(\cdot)$, to be $A$ we get, $|A| \geq (n+1)^{|X|}$.

Thus using Lemma 1 and equations (13) and (15) we get,
\[ w(A) \geq v(A_\epsilon)^{\beta} e^{-n(D(V_{\rho}[W|x]|P) + \epsilon(\beta, n))} \quad (16a) \]
\[ v(A) \geq 1 - \frac{1}{|A| - 1} \sum_{\mathcal{M}} e^{n(D(V_{\rho}[Q_{\rho}|P) - \epsilon(\beta, n))} \quad (16b) \]

3Using techniques similar to those in [1], see Appendix A for details.

4The details of the bound on the variance are presented in Appendix B.
where \( \epsilon_2(\beta, n) = \beta[(\ln(1 + n)) + 4/\beta^2] + \frac{[\gamma_1(1 + n)]}{n} \)

There exists a parametric family of \( Q_\rho(\cdot) \)'s which is continuous in \( \rho \), see [6] or appendix D for details, such that,

\[
\ln r_p(x) \geq -\frac{E_0(\rho)}{1 + \rho} \tag{17}
\]

Furthermore when all entries of \( W(\cdot) \) is positive, \( \delta_{Q_\rho} \geq \delta_W \) for all \( \rho \). Using equations (12) and (17) we get,

\[
\mathcal{D}(V_\rho || W|P) \leq E_0(\rho) - \rho \mathcal{D}(V_\rho || Q_\rho|P) \quad \forall P, \rho \tag{18}
\]

Note that for any \( P \),

\[
\text{either} \quad \mathcal{D}(V_\rho || Q_\rho|P)|_{\rho = \rho^*} = R - \epsilon_2(\beta, n) - \frac{(1 + \beta) \ln 2}{\beta n} \tag{a} \\
\text{or} \quad \mathcal{D}(V_\rho || Q_\rho|P)|_{\rho = \rho^*} > R - \epsilon_2(\beta, n) - \frac{(1 + \beta) \ln 2}{\beta n} \tag{b}
\]

If (a) is the case: using (12) and (16) at \( \rho = 0 \) we get

\[
w(A_\rho) \geq \left(\frac{1}{2}\right)^{|\rho|} e^{-n\epsilon_2(\beta, n)} \tag{19}
\]

If (b) is the case: note that \( \lim_{\rho \to \infty} \mathcal{D}(V_\rho || Q_\rho|P) = 0 \). Thus, by the intermediate value theorem, there exist some \( \rho^*_p \) such that \( \mathcal{D}(V_\rho || Q_\rho|P)|_{\rho = \rho^*_p} = R - \epsilon_2(\beta, n) - \frac{(1 + \beta) \ln 2}{\beta n} \). Using equations (16) and (18) at \( \rho = \rho^*_p \), together with the fact that \( E_{\exp}(R) \geq E_0(\rho) - \rho \mathcal{D}(V_\rho || P_\rho) \geq 0 \) we get

\[
w(A_\rho) \geq \left(\frac{1}{2}\right)^{|\rho|} e^{-n\epsilon_2(\beta, n)} \tag{20}
\]

Equation (11) follows equations (19) and (20) and the identity \( \ln \frac{1}{\beta n} + \frac{1}{2} + 2 \ln 2 \leq \ln \frac{1}{\beta n} \) by setting \( \beta = n^{-1/2} \).

Notice that, when there is feedback, the input letter at any time \( t \) for any message \( m \) depends on the previous channel outputs. Thus, we can not

- claim conditional independence of \( Y_t \)'s or equation (13).
- make an expurgation over types

However for the particular encoding schemes satisfying the assumption 5 we can address both of the issues. For doing that we need to analyze the mixing properties of Markov chains resulting from \( \Gamma \) and \( \Phi \) for each \( m \in M \) under \( v(\cdot) \).

IV. FINITE STATE MACHINE ENCODERS AND MIXING

Let \( v(\cdot) \) and \( q(\cdot) \) be of the form given in (7) for some channel output probability distribution \( Q(\cdot) \), and some transition probabilities \( V(\cdot) \). Then, for encoding schemes with feedback we can not write (13), because the channel outputs are not conditionally independent given the message. However, when (5) holds, the dependence between \( y_t \) and \( y_v \) vanishes as \( t - u \) increases. Lemma 2 below uses this property to bound the terms \( E_v[\exp(\beta \mu_u^t)] m, s_u \) and \( E_v[\exp(\beta \nu_u^t)] m, s_u \), where

\[
\mu_u^t := \ln \frac{v(y_u^t|m, s_u)}{w(y_u^t|m, s_u)} \quad \nu_u^t := \ln \frac{q(y_u^t|m, s_u)}{q(y_u^t|m, s_u)} \tag{21}
\]

The upper bound provided is in terms of the empirical type

\[
P_m^s(x) := \frac{1}{t - u} \sum_{j = u}^{t} v(\Phi_j(m, s_j) = x|m, s_u = s^*) \tag{22}
\]

for any \( s^* \in S \). Observe that, in contrast to the case without feedback, the type \( P_m^s(\cdot) \) depends on the particular \( V(\cdot) \) that is used. However, this will not prevent one from applying the intermediate value theorem, in virtue of the continuity of \( \mathcal{D}(V||W|P) \) in \( P \).

**Lemma 2:** For any feedback encoder of the form (4), satisfying (5), \( u \leq t \), \( s^* \in S \), \( \beta \in (0, \frac{\ln \max\{4\mu^t, \delta_V^k\}}{t - u + 1}) \),

\[
E_v[\exp(\beta \mu_u^t)] m, s_u \leq (t - u + 1)E_v[\mathcal{D}(V||W|P) + \delta_V^k] \tag{23a}
\]

\[
E_v[\exp(\beta \nu_u^t)] m, s_u \leq (t - u + 1)E_v[\mathcal{D}(V||Q_{\rho^*}|P) + \delta_V^k] \tag{23b}
\]

where \( \epsilon_3 := \frac{k \ln \delta_1 + e^{-1}}{2} \).

**Proof:** If \( z \in E[z] \leq 1 \) with probability one, then

\[
E[\exp(z)] \leq \exp(E[z] + E[\{-z - E[z]\}^2]).
\]

Hence, if \( \beta \leq -((t - u + 1)^{-1}) \ln \delta_V^k \), then

\[
E_v[\exp(\beta \mu_u^t)] m, s_u \leq \exp[\beta E_v[\mu_u^t] m, s_u + \epsilon_4], \tag{24}
\]

where \( \epsilon_4 := 2(t - u + 1)\beta \delta_V^{-2k}(k \ln \delta_1 + e^{-1}) \ln(\delta_V^{-1}) \). Now, we consider \( E_v[\mu_u^t] m, s_u \) and bound its dependence on \( s_u \). Observe that, conditioned on \( m \) and \( s_u \), the state sequence \( s_u \) forms a Markov chain on \( S \) whose time-dependent transition probabilities are given by

\[
\Pi_j(s_{j+1}|s_j) := \sum_{y_{j+1}} V(y|\Phi(m, s_j)) \quad \forall u \leq j < t.
\]

Let us consider a copy of this Markov chain, \( s_u^t \), which starts at time \( u \) in \( s_u^t = s^* \), evolves independently from \( s_u^t \), according to the same transition kernel \( \Pi_j(\cdot) \) until the first time they meet, and sticks to it thereforth. Let \( \mu_{u}^t \) be defined as in (21) with \( s_u^t \) replacing \( s_u \), and notice that

\[
P_v\{s_{u+k} = s_{u+k}|m, s_t, s_{t+k}\} \leq \delta_V^k.
\]

As a consequence,

\[
P_v\{s_{u+k} \neq u+i+k|m, s_u\} \leq (1 - \delta_V^k)^i, \quad i \geq 0.
\]

Using the fact that \( \mu_{u+k}^t \leq k \ln \delta_V^{-1} \), and the inequality \( -x \ln x \leq e^{-1} \), one gets, for \( \gamma = k \ln \delta_V^{-1} + e^{-1} \)

\[
E_v[\mu_{u+k}^t] m, s_u \leq \gamma(1 - \delta_V^k)^i \tag{27}
\]

Using equations (26) and (27) , we get

\[
E_v[\mu_u^t - \mu_{u}^t] m, s_u \leq \sum_{i=0}^{(t-u+1)/k} \gamma(1 - \delta_V^k)^i \tag{a}
\]

Using equations (25) and (28)

\[
E_v[\mu_u^t] m, s_u \leq (t - u + 1)D(V||W|P) + \gamma \delta_V^{-k} \tag{29}
\]

Then, (23a) follows from (24), and (29). Equation (23b) can be derived from a similar discussion. ■

—See Appendix A for details.

—Details of the bound on \( E_v[\mu_u^t - \mu_{u}^t] m, s_u \) are presented in Appendix C.
V. SUPER-LETTERS AND FIXED COMPOSITION ARGUMENT

Notice that, as a result of Lemma 2, we know that the dependence of both $E_p[\exp(\beta f_{\mu_0})] m, s_u]$ and $E_p[\exp(\beta f_{\mu_0})] m, s_u]$ on $s_u$ tends to fade away, as $(t-u)$ grows large. On the other hand, if $(t-u)$ is large but finite, one can interpret $(t-u)$-long encoding functions together with $(t-u)$-long sequences of $\Gamma_i$, as input letters and make a fixed composition argument to bound $E_p[\exp(\beta f_{\mu_0})] m, s_1]$ and $E_p[\exp(\beta f_{\mu_0})] m, s_1]$. The rest of this section is devoted to making this argument precise and establishing the bound given in Theorem 1, using Lemmas 1 and 2.

First notice that for any $t \in [1,n]$ and $m \in M$, $\Gamma_t$ is a mapping from $S \times Y$ to $\Sigma$, i.e. an element of $S^S \times Y$. Thus for any $m \in M$ any $t$-long string of $\Gamma$ and $\Phi(m)$, say $(\Gamma_{t+1},\Phi_{t+1}(m))$, is a function $S \times Y \times \mathcal{X}$ of $Z$. If we interpret $t$-long parts of the encoding function and finite state machine, $(\Gamma_{t+1},\Phi_{t+1}(m))$, as super-letters, $\alpha_i$ for $i = 0,1,\ldots,([\frac{t}{\ell}] - 1)$ then the codeword for a message $m \in M$ is composed of $\frac{t}{\ell}$ super-letters and an $(m - \frac{t}{\ell})\ell$ long extension. Including different extensions are less than $(\frac{t}{\ell} + 1) |\mathcal{X}| |S|^{|\mathcal{X}}|^{t}$ different types. Thus if we choose $\alpha$ to be the most populous type we will have

$$|\alpha|^{|\mathcal{X}}| \geq \exp(-(|S|^{|\mathcal{X}}|)|S|^{|\mathcal{X}}| |\mathcal{X}|)^{\ln(1+\frac{t}{\ell})} - |S|^{|\mathcal{X}}| |\mathcal{X}|^{t} \quad (30)$$

Note that codewords of the message in set $\alpha$ differ only in first $n_1 = \ell([\frac{t}{\ell}] - 1)$ time instances. Although ordering of these super-letters will effect the actual value of $E_p[\exp(\beta \ln \frac{v(y^{n_1}m)}{l(y^{n_1}m)}) m]$ and $E_p[\exp(\beta \ln \frac{v(y^{n_1}m)}{l(y^{n_1}m)}) m]$, we can bound all of those expectations in a way that is independent of the ordering, using Lemma 2. As a consequence, for $\beta \in [0, -\ln \min_{x \in E}(z(x))]$,

$$E_p[\exp(\beta \ln \frac{v(y^{n_1}m)}{l(y^{n_1}m)}) m] = e^{\beta n_1(D(V||W)\parallel P_m) - e_{5}} \quad (31a)$$

$$E_p[\exp(\beta \ln \frac{v(y^{n_1}m)}{l(y^{n_1}m)}) m] = e^{\beta n_1(D(V||Q)\parallel P_m) - e_{5}} \quad (31b)$$

where $e_{5} = \left(\frac{\ln 2}{2}\right) - e^{-1} + \left(\frac{1}{2} + 2\beta \ln \frac{2}{m}\right)$ and

$$P_m(x) = \frac{\sum_{m=1}^{m} \sum_{m'=1}^{m} P(X_{m'=1}^{x} = x|m,s_{m'=1}^{m}=j)}{n_1} \quad (32)$$

Note that unlike $P_m$ in the non-feedback case $P_m$ in equation (32) depends on $V$. However that dependence is continuous in $V$. Furthermore $P_m$ is identical for all messages in a given type, no matter what $V$ is.

As we did in the non-feedback case we will use $V_{\rho}$ and $Q_{\rho}$ and use equation (18). Using equations (30) and (31) together with Corollary 1 we get

$$w(A_{\rho}) \geq v(A_{\rho}) \frac{e^{\beta n_1(D(V_{\rho}\parallel W)\parallel P_{\rho})}}{e_{6}} \quad (33a)$$

$$v(A_{\rho}) \geq 1 - e^{-\frac{\beta}{m}}(D(V_{\rho}\parallel Q_{\rho})\parallel P_{\rho} - e_{6} - \frac{1}{2} R) \quad (33b)$$

where $e_{6} = \epsilon_{5} + \ln(S^{|S|^{|\mathcal{X}}|}|S|^{|\mathcal{X}|}/|\mathcal{X}|)^{\ln(1+\frac{t}{\ell})} - |S|^{|\mathcal{X}}| |\mathcal{X}|^{t}$.

Note that both $V_{\rho}$ and $Q_{\rho}$ are continuous functions of $\rho$. Hence, $P_m$ is a continuous function of $\rho$. As a consequence, $D(V_{\rho}\parallel Q_{\rho})\parallel P_{m}$ is continuous in $\rho$. Thus, $D(V_{\rho}\parallel Q_{\rho})\parallel P_{m}$ is either less than, or strictly greater than $\frac{1}{m} R - e_{6} + \frac{1}{2} R$.

Using the same reasoning as in the non-feedback case, one gets that, for $\beta \in [0, -\ln \min_{x \in E}(z(x))]$,

$$w(A_{\rho}) \geq \left(\frac{1}{2}\right) \frac{e^{\beta n_1(D(V_{\rho}\parallel R - e_{6} + \frac{1}{2} R)}}{e_{6}} \quad (34)$$

Note that when all entries of $W$ are positive $\delta_{Q_{\rho}} \geq \delta_{W}$ and $\delta_{V_{\rho}} \geq \delta_{W}$. Using equation (34) and setting $\beta = \frac{1}{2 e}\frac{1}{2 (1 - \ln \delta_{W})}$ and using the fact that $exp(\cdot)$ is decreasing function of its argument we recover equation (6).

VI. DISCUSSION

In this paper, we have proved a lower bound on the error probability of fixed-length block-codes with finite state machine encoders over discrete memoryless channels with feedback. We have shown that, when the transmitter is only allowed to store the feedback information by means of a finite state machine, whose is updated as channel outputs are fed back to it, the sphere-packing bound continues to hold even on non-symmetric DMCs. Ongoing work includes relaxing some of the technical assumptions, and extending our results to channels with memory.

ACKNOWLEDGMENTS

The work leading to this manuscript has grown out of several conversations between the authors and Harikrishna R. Palaiyanur and Prof. Anant Sahai of Berkley, Prof. Sekhar Tatikonda of Yale, and Prof. Sanjoy Mitter of MIT.

APPENDIX

A. $E[\exp(z)] = \exp(E[z])$:

Let $g(z) = 2e^{\frac{z-1}{z}}$ than one can show that

$g(z) \geq 0 \quad g'(z) \geq 0 \quad g''(z) \geq 0$.

Let $z$ be r.v. such that $z - E[z] \leq 1$ then,

$$E[\exp(z - E[z])] = E \left[ 1 + z - E[z] + \frac{(z - E[z])^2}{2} \right]$$

$$\leq 1 + E \left[ \frac{E(z - E[z])^2}{2} \right]$$

$$\leq \exp \left( \frac{E(z - E[z])^2}{2} \right).$$

Using $g(1) \leq 1$ we get,

$$E[\exp(z)] \leq \exp(E[z] + E[z^2] - E[z^2]) \quad (35)$$

B. Bounding $\sum_y f_y (\ln \frac{f_y}{g_y})^2 - (\sum_y f_y \ln \frac{f_y}{g_y})^2$:

Let $f_y$ and $g_y$ be two probability distributions on $Y$ then

$$\sum_y f_y (\ln \frac{f_y}{g_y})^2 \leq \sum_y g_y \frac{f_y}{g_y} (\ln \frac{f_y}{g_y})^2 \leq \sum_y g_y \sum_y \left( \frac{f_y}{g_y} (\ln \frac{f_y}{g_y})^2 \right) \leq (\frac{f_y}{g_y})^2 + \frac{1}{2} \leq \left( \frac{f_y}{g_y} \right)^2 + \frac{1}{2}$$

(36)
where in step (a) we used the facts that $f_y \leq 1$, $g_y \geq \delta_y$ and $x(\ln x)^2 \leq \frac{1}{x}$ for $x \in [0, 1]$. Thus

$$
\sum_y f_y (\ln g_y)^2 - (\sum_y f_y \ln g_y)^2 \leq (\frac{1}{\ln g_y})^2 + \frac{4}{x^2} \tag{37}
$$

C. Bounding $E_v \left[ (\mu'_u - \mu_u)^2 \mid m, s_u \right]$

Let us denote $E_v \left[ (\mu'_u - \mu_u)^2 \mid m, s_u \right]$ by $\mu_t'$ for brevity.

$$
E_v \left[ (\mu'_u - \mu_u)^2 \mid m, s_u \right] = \sum_{j=t}^\infty E_v \left[ (\mu_j - \mu_t')^2 \mid m, s_u \right] + \sum_{j=t}^{t-1} E_v \left[ (\mu_j - \mu_j')(\mu_{j+1} - \mu_{j+1}') \mid m, s_u \right] \tag{38}
$$

Note that

$$
E_v \left[ (\mu_j - \mu_t')^2 \mid m, s_u \right] = E_v \left[ (\mu_j)^2 \mid m, s_u \right] = E_v \left[ E_v \left[ (\mu_j)^2 \mid m, s_t \right] \mid m, s_u \right] \leq (\ln \delta_W)^2 + 4e^{-2} \tag{39}
$$

the inequality following from (36). For $u \leq j < t$, it holds

$$
E_v \left[ (\mu_j - \mu_t')^2 \mid m, s_u \right] = E_v \left[ (\mu_j - \mu_t')^2 \mid m, s_u \right] + E_v \left[ (\mu_j - \mu_t') \left( E_v \left[ (\mu_{j+1})^2 \mid m, s_j+1 \right] \mid m, s_u \right) \right] \leq E_v \left[ (\mu_j - \mu_t')^2 \mid m, s_u \right] \tag{40}
$$

where (a) follows from the Markovian property of the encoding and (b) follows from Schwartz’s inequality. In addition, as a result of the Markovian property, we have

$$
\mu_t' = E_v \left[ (\mu_t')^2 \mid m, s_t \right] \tag{41}
$$

Using equation (29) together with equation (41) we get,

$$
E_v \left[ (\mu'_u - \mu_u)^2 \mid m, s_u \right] - \mu_t' \leq \delta_V^{2k}(-k \ln \delta_W - e^{-1}) \tag{42}
$$

Using equation (38), (39), (40) and (42) and the fact that $\ln \delta_W^2 + 4e^{-2} \leq \ln \left( e/\delta_W \right)$ we get,

$$
E_v \left[ (\mu'_u - \mu_u)^2 \mid m, s_u \right] \leq (t-u+1) \left( \frac{k \ln \frac{\delta_W}{\delta_V} - e^{-1}}{\delta_V^2} + \ln \frac{\delta_V}{\delta_W} \right) \ln \frac{\delta_V}{\delta_W} \tag{43}
$$

D. Uniqueness and Continuity of $Q_\rho$

Recall that

$$
e^{-E_0(\rho,Q)} = \min_x \sum_y W(y|x) \frac{1}{1+\rho} Q(y)^{1+\rho} \tag{39}
$$

$$
e^{-E_0(\rho, Q)} = \max_{Q_\rho} e^{-E_0(\rho,Q)} \tag{40}
$$

Note that maximizing $Q_\rho$ satisfies

$$
\sum_y W(y|x) \frac{1}{1+\rho} Q_\rho(y)^{1+\rho} \geq e \frac{E_0(\rho)}{1+\rho} \quad \forall x \tag{44}
$$

and with equality for some $x$.

Note that if there are two distinct optimal distributions $Q_{\rho,a}$ and $Q_{\rho,b}$ then

$$
\sum_y W(y|x) \frac{1}{1+\rho} Q_{\rho,a}(y)^{1+\rho} + (1-\alpha)Q_{\rho,b}(y)^{1+\rho} \geq \sum_y W(y|x) \frac{1}{1+\rho} (\alpha Q_{\rho,a}(y) + (1-\alpha)Q_{\rho,b}(y))^{1+\rho} \tag{45}
$$

All of their linear combinations will lead to a strictly larger $E_0(\rho)$ so they can not be the optimal $Q_\rho$ simultaneously. Thus there exist a unique $Q_\rho$.

Note that $e^{-E_0(\rho,Q)}$ is a decreasing function for all decreasing in $\rho$. Because

$$
E \left[ x^{1+\rho} \right]^{1+\rho} = E \left[ x^{-1+\rho} (\frac{1}{x})^{1+\rho} \right] \geq \frac{E \left[ x^{-1+\rho} \right]}{(1+\rho)^{1+\rho}} \tag{46}
$$

for $\rho' \geq \rho$. Then $e^{-E_0(\rho)}$ is also a decreasing function of $\rho$.

Thus

$$
0 \leq e^{-E_0(\rho)} - e^{-E_0(\rho+\epsilon)} \leq e^{-E_0(\rho,Q_\rho)} - e^{-E_0((\rho+\epsilon),Q_\rho)} \tag{47}
$$

$$
0 \leq e^{-E_0(\rho)} - e^{-E_0(\rho+\epsilon)} \leq \delta_1(Q_\rho, \epsilon) \tag{48}
$$

where $\lim_{\epsilon \to 0} \delta_1(Q_\rho, \epsilon) = 0$. Last step follows from the continuity of $e^{-E_0(\rho,Q)}$ in $\rho$ for any $Q$.

Furthermore

$$
e^{-E_0(\rho)} - e^{-E_0(\rho+\epsilon)} \geq e^{-E_0(\rho,Q_\rho)} - e^{-E_0(\rho,Q_{\rho+\epsilon})} \tag{49}
$$

$$
\geq \zeta(\|Q_\rho - Q_{\rho+\epsilon}\|) \tag{50}
$$

where the $\zeta(\rho)$ is strictly increasing function such that $\zeta(0) = 0$. Last step follows from the strict convexity of $-e^{-E_0(\rho,Q)}$ in $Q$.

Thus as result of equations (45) and (46) we get,

$$
\|Q_\rho - Q_{\rho+\epsilon}\| \leq \zeta^{-1}(\delta_1(Q_\rho, \epsilon)) \tag{51}
$$

$$
\lim_{\epsilon \to 0} \delta_1(Q_\rho, \epsilon) = 0 \text{ and } \zeta^{-1}(\cdot) \text{ is also a strictly increasing function such that } \zeta^{-1}(0) = 0. \text{ Thus } Q_\rho \text{ is continuous in } \rho.
$$

REFERENCES


