The Capacity of Channels with O(1)-Bit Feedback

Eric Ruzomberka*, Yongkyu Jang†, David J. Love† and H. Vincent Poor*
*Princeton University †Purdue University

2023 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-7554-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIT54713.2023.10206714

***Abstract*—We consider point-to-point communication with partial noiseless feedback in which the number of feedback bits is $O(1)$ in the number of transmitted symbols. For $q \geq 2$, we study the general q-ary alphabet setting with both errors and erasures and seek to characterize the zero-error capacity. As our main result, we provide a tight characterization of zero-error capacity which we prove via novel achievability and converse schemes inspired by the study of causal/online adversarial channels without feedback. Perhaps surprisingly, we show that $O(1)$-bits of feedback are sufficient to achieve the zero-error capacity of the error channel with full noiseless feedback when the fraction of transmitted symbols in error is sufficiently small.**

I. Introduction

One of the oldest questions in coding theory is, "What is the impact of transmitter feedback on the fundamental limits of reliable communication?" Shannon addressed this question in his 1956 paper [1], in which he showed that feedback does not increase channel capacity for a point-to-point memoryless channel. In the same work, Shannon conversely showed that feedback can increase the zero-error capacity when the channel noise is modeled in a worst-case manner. Since Shannon's work, a large body of research has studied the zero-error capacity problem for various channel models with feedback, producing a number of capacity characterizations along with constructive coding schemes which can achieve capacity with remarkable simplicity [2]–[4].

A notable drawback of the above coding schemes are their dependency on *full noiseless feedback* for which the transmitter observes a noiseless and undelayed version of the channel output after every transmitted symbol. Motivated by the fact that feedback is a costly resource, recent work [5] has initiated the study of the *partial noiseless feedback* setting in which feedback is only sent after a fraction $\delta \in (0, 1]$ of all transmitted symbols. Consider a channel model with a q-ary input alphabet $\mathcal{X} = \{0, 1, \ldots, q-1\}$ for some $q \geq 2$, where a fraction $p \in [0, 1]$ of all transmitted symbols are received in error. For binary alphabets (i.e., $q = 2$), a result of [5] is that the zero-error capacity is positive for all $p \in [0, 1/3)$ when $\delta \in (2/3, 1]$.[1] More recently, [7] improved upon this result and showed that for n transmitted bits, just $O(\log n)$ bits of feedback is sufficient to achieve some positive rate for all $p \in [0, 1/3)$, while for $p > 1/4$ the zero-error capacity is 0 when the number of feedback bits is $o(\log n)$. *Hence, when $o(\log n)$ bits of feedback are available, the support of the zero-error capacity coincides with the support when no feedback is available.*[2]

In light of this negative result, one may wonder if $o(\log n)$ bits of feedback are still useful from a capacity point-of-view. The extent to which feedback is used in real-world communication systems suggests that it may be too costly to require that the number of feedback bits scale in n. Indeed, feedback is often restricted to a few bits per transmission block, e.g., in LTE/5G feedback-supported protocols such as hybrid-ARQ, channel precoding for multi-antenna wireless, and CSI usage [9]. In this work, we consider a more limited form of partial noiseless feedback than [5]–[7] in which the number of feedback bits is $O(1)$ i.e., does *not* grow with the number of transmitted symbols n. We consider the general q-ary setting under both symbol errors and symbol erasures, and show that $O(1)$-bit feedback can increase the zero-error capacity compared to the setting when no feedback is available.

Our setting is roughly as follows. (See Section II for detailed definitions). A sender (Alice) wishes to communicate a message m from a message set $\mathcal{M}$ to a receiver (Bob) by transmitting a sequence of symbols from a q-ary input alphabet $\mathcal{X} = \{0, 1, \ldots, q-1\}$. For rate $R = \frac{1}{n}\log_q |\mathcal{M}|$ and $B \geq 0$ bits of partial noiseless feedback, an (n, Rn, B)-code is a scheme that makes n transmissions in the *forward channel* (i.e., from Alice to Bob) and at most B transmissions comprising a total of B bits in the *reverse channel* (i.e., from Bob to Alice).[3] Prior to communication, Alice and Bob choose an (n, Rn, B)-code for communication, while during communication, the forward channel induces pn symbol errors and rn symbol erasures.[4] A rate R is said to be *(zero-error) achievable with $O(1)$-bit feedback* if there exists a constant $B \geq 0$ and for large enough n there exists an (n, Rn, B)-code that allows Alice to communicate any message $m \in \mathcal{M}$ to Bob without decoding error. The zero-error capacity, denoted $C_q(p, r)$, is the supremum of rates achievable with $O(1)$-bit feedback.

A. Results

In this work, we study the zero-error capacity $C_q(p, r)$ for the q-ary error/erasure channel with $O(1)$-bit feedback. As our main result, we present a complete characterization of

This work is supported in part by the U.S National Science Foundation under Grants CCF-1908308, CNS-2212565, CNS-2225577, ITE-2226447 and EEC-1941529 and in part by the Office of Naval Research.

[1] This result was extended in [6] to the q-ary setting for $q \geq 3$.

[2] For binary alphabets without feedback, by the Gilbert-Varshamov bound, some positive rate is achievable for any $p \in [0, 1/4)$. Conversely, by the Plotkin bound [8], no positive rate is achievable for $p \geq 1/4$.

[3] Setting $B = (n-1)\log_2(q+1)$ corresponds to full noiseless feedback. That is, this setting corresponds to a feedback set of size $2^{(n-1)\log_2(q+1)} = (q+1)^{n-1}$, i.e., one q-ary symbol or erasure symbol of feedback per channel use.

[4] We assume noiseless feedback such that no errors or erasures occur on the reverse channel.

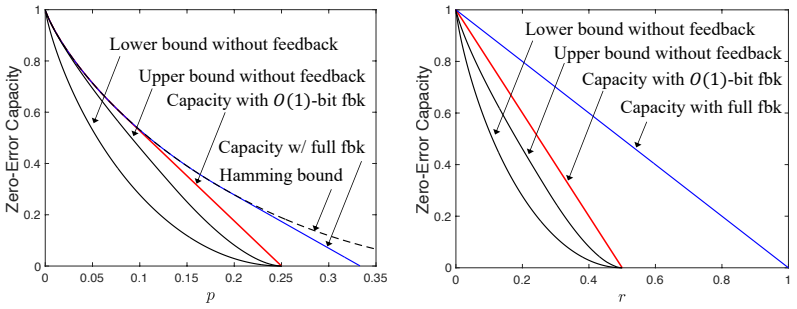

Fig. 1: Zero-error capacity bounds of (a) binary error channels and (b) binary erasure channels. Red plots show the capacity $C_2(p,r)$ of binary channels with $O(1)$-bit feedback (Thm. 1). The capacity of the channel without feedback has best known lower bounds and upper bounds given by the GV bound [10], [11] and MRRW bound [12], respectively. The capacity $C_2^{\text{full}}(p,0)$ of the error channel with full feedback is given by Berlekamp [2] and Zigangirov [3]. The dashed plot shows the Hamming bound $1-H_2(p)$.

$C_q(p,r)$. Our proof of this result involves a novel coding scheme which allows us to prove a lower bound on $C_q(p,r)$ and a converse analysis which allows us to prove a matching upper bound on $C_q(p,r)$, both of which are inspired from prior work [13]–[15] on causal channels without transmitter feedback (see Section I-B for a detailed discussion). Due to space limitations, we leave the proof of the lower bound for the extended version. For $q \geq 2$, denote the q-ary entropy function as $H_q(x)$, which is equal to $H_q(x) = x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ for $x \in [0,1]$.

Theorem 1. *Suppose that $q \geq 2$, $p \in [0,1]$ and $r \in [0,1]$. The zero-error capacity of the q-ary symbol error/erasure channel with $O(1)$-bit feedback is*

$$C_q(p,r) = \begin{cases} \min\limits_{\bar{p}\in[0,p]} \left[\alpha(\bar{p})\left(1 - H_q\left(\frac{\bar{p}}{\alpha(\bar{p})}\right)\right)\right], & 2p + r < \frac{q-1}{q} \\ 0, & \text{otherwise} \end{cases}$$

where $\alpha(\bar{p}) = 1 - \frac{2q}{q-1}(p-\bar{p}) - \frac{q}{q-1}r$.

We remark that in our achievability proof of Theorem 1, our coding scheme uses a the number of feedback bits B that varies with the coding rate. For fixed $p \in [0,1]$, $r \in [0,1]$ and $q \geq 2$, our coding scheme of rate $R < C_q(p,r)$ uses a number of feedback bits B which tends to infinity as the rate-to-capacity gap $\epsilon_R = C_q(p,r) - R$ tends to 0.

To better understand the capacity expression in Theorem 1, we focus on two special cases: when the channel can only induce errors (i.e., $p \in [0,1]$ and $r = 0$) and when the channel can only induce erasures (i.e., $p = 0$ and $r \in [0,1]$). These special cases are plotted in Fig. 1 for binary alphabets. For general alphabets $q \geq 2$, the capacity expression in Theorem 1 can be simplified. When only erasures occur, $C_q(0,r)$ is equal to $1 - \frac{q}{q-1}r$ for $r \in [0, \frac{q-1}{q})$ and 0 for $r \in [\frac{q}{q-1}, 1]$. When only errors occur, for $p \in [\frac{q-1}{2q}, 1]$ it is easy to verify that $C_q(p,0) = 0$, and for $p \in [0, \frac{q-1}{2q})$, $C_q(p,0)$ is equal to the Hamming bound $1 - H_q(p)$ for small p and is otherwise equal to the line tangent to $1 - H_q(p)$ and which intersects the point $(p,0)$ where $p = \frac{q-1}{2q}$.

We compare the above result to the setting with full (noiseless) feedback. The zero-error capacity of the q-ary error/erasure channel with full feedback, denoted $C_q^{\text{full}}(p,r)$, is the largest rate R for which there exists an $(n, Rn, (n-1)\log_2(q+1))$-code that allows Alice to communicate any message $m \in \mathcal{M}$ to Bob without decoding error. By definition, it is clear that $C_q^{\text{full}}(p,r)$ is an upper bound of $C_q(p,r)$. We briefly summarize known characterizations of $C_q^{\text{full}}(p,r)$. In the binary case, a complete characterization of $C_2^{\text{full}}(p,0)$ for all $p \in [0,1]$ was provided by Berlekamp [2] and Zigangirov [3]. For $q \geq 3$, a result of Ahlswede, Deppe and Lebedev [4] is the upper bound

$$C_q^{\text{full}}(p,0) \leq \begin{cases} 1 - H_q(p), & p \in [0, \frac{1}{q}) \\ (1-2p)\log_q(q-1), & p \in [\frac{1}{q}, \frac{1}{2}) \end{cases} \quad (1)$$

and $C_q^{\text{full}}(p,0) = 0$ for $p \in [\frac{1}{2}, 1]$ which is tight for all $p \in [1/q, 1]$.[5] However, for $q \geq 3$ and $p \in [0, 1/q]$, a tight characterization of $C_q^{\text{full}}(p,0)$ remains open. A corollary of Theorem 1 is that that the upper bound (1) is tight for small values of p.

Corollary 1.1 (Full Feedback)**.** *Suppose $q \geq 2$. The capacity of the q-ary error channel with full feedback is*

$$C_q^{\text{full}}(p,0) = C_q(p,0) = 1 - H_q(p), \quad p \in (0, p^*]$$

where $p^* \in [0, \frac{q-1}{2q}]$ is the unique value that satisfies equation $p^*(1-p^*)^{\frac{q+1}{q-1}} = (q-1)q^{-\frac{2q}{q-1}}$. Proof is in the extended version.

We reiterate that for $q \geq 2$ and for $p \in (0, p^*)$, the zero-error capacity with full feedback $C_q^{\text{full}}(p,0)$ can be achieved with some coding scheme that uses only $O(1)$-bit feedback. While a scheme using $O(1)$-bit feedback cannot be used to achieve $C_q^{\text{full}}(p,0)$ for $p \in [p^*, 1]$, the following corollary implies that such a scheme can achieve rates close to $C_q^{\text{full}}(p,0)$ for all $p \in [0,1]$ when the alphabet size q is large.

Corollary 1.2 (Large Alphabets)**.** *Suppose that $p \in [0,1]$ and $r \in [0,1]$. If $2p + r < 1$ then*

$$C_q(p,r) = 1 - 2p - r - \Theta\left(\frac{1}{q}\right) \text{ as } q \to \infty.$$

Otherwise, if $2p + r \geq 1$ then $C_q(p,r) = 0$ for all $q \geq 2$. Proof is in the extended version.

We remark that for $2p + r < 1$, both letters $C_q(p,r)$ and $C_q^{\text{full}}(p,r)$ tend to the same limit $1 - 2p - r$ as q tends to

[5] We remark that the coding scheme proposed in [4] to achieve $C_q^{\text{full}}(p,0)$ for $p \in [1/q, 1/2)$ uses full (noiseless) feedback. The authors of [4] refer to their scheme as the 'rubber method'.

∞, albeit at different rates. $C_q(p,r)$ tends to the limit slightly slower than $C_q^{\text{full}}(p,r) = 1-2p-r-\Theta\left(\frac{1}{q\log q}\right)$. Conversely, $C_q(p,r)$ tends to the limit $1-2p-r$ faster than the best known lower bound on the zero-error capacity without feedback $1-2p-r-\Theta(\frac{1}{\sqrt{q}})$ due to Tsfasman, Vlăduts and Zink[6] [16].

B. Related Work

As discussed above, our study of channels with $O(1)$-bit feedback is related to prior studies on channels with full feedback [2]–[4] and partial feedback [5]–[7]. More generally, our study is related to *adversarial channels* – a channel modeling framework in which the channel noise is chosen by a malicious adversary seeking to disrupt communication. Adversarial channels may be modeled with or without feedback, and include myopic channels [17]–[19], arbitrarily varying channels (AVCs) [6], [20], and causal adversarial channels [13]–[15], [21], [22]. We remark that the q-ary channel with $O(1)$-bit feedback is an adversarial channel when studied under a zero-error capacity setting.

Among the above adversarial channel models, causal adversarial channels (without transmitter feedback) have a particularly close connection to channels with $O(1)$-bit feedback. A channel is said to be *causal* if the adversary's choice to induce an error/erasure in the ith transmitted symbol depends only on previously transmitted symbols, i.e., symbols 1 through $i-1$. One connection between the two models, which appears at first glance to be coincidental, is that the bounded-error capacity of the q-ary error/erasure causal channel [15] coincides exactly with the zero-error capacity of the q-ary error/erasure channel with $O(1)$-bit feedback (Theorem 1). The authenticity of this connection becomes apparent in our proof of Theorem 1, which uses insights and tools developed in the study causal adversarial channels to prove both a lower bound (achievability) and a tight upper bound (converse) of $C_q(p,r)$.

Our converse proof is based on the so called "babble-and-push" adversarial attack of [13], [15] where it was proposed to study upper bounds on the capacity of causal adversarial channels without transmitter feedback. In the converse analysis, "babble-and-push" is an attack strategy used by an adversary to confuse Bob about Alice's transmitted codeword. A key step in the converse analysis is to bound the number of codewords within a specified Hamming distance using the Plotkin bound. We propose a novel extension of the standard "babble-and-push" framework to incorporate $O(1)$-bit feedback by using ideas from Ramsey theory. Furthermore, our achievability proof uses a novel coding scheme that resembles the capacity achieving scheme of [14], [15]. Due to space limitations, we leave the achievability proof for the extended paper.

II. Channel Model

A. Notation

For integer $q \geq 2$, define $\mathcal{Q} = \{0,1,\ldots,q-1\}$. For an integer $n \geq 0$, the notation $[n]$ denotes the set $\{1,2,\ldots,n\}$. For two sequences $\boldsymbol{a},\boldsymbol{b} \in \mathcal{Q}^n$, the Hamming distance $d_H(\boldsymbol{a},\boldsymbol{b})$ between $\boldsymbol{a}$ and $\boldsymbol{b}$ is usually defined as the number of positions $i \in [n]$ in which $a_i \neq b_i$. We extend this definition of Hamming distance to account for sequences containing the erasure symbol '?' by defining the distance $d_H(\boldsymbol{a},\boldsymbol{b})$ between the sequences $\boldsymbol{a} \in \mathcal{Q}^n$ and $\boldsymbol{b} \in \{\mathcal{Q} \cup \{?\}\}^n$ to be the number of positions $i \in [n]$ in which $b_i \neq ?$ and $a_i \neq b_i$.

[6]The lower bound of [16] follows from the study of algebraic geometry codes and only holds for $q \geq 49$ and when $\sqrt{q}$ is an integer. For general q, the best known lower bound on the zero-error capacity without feedback is the Gilbert-Varshamov bound [10], [11].

B. Channel Model

For $q \geq 2$, the channel is characterized by an input alphabet $\mathcal{X} = \mathcal{Q} \triangleq \{0,1,\ldots,q-1\}$, an output alphabet $\mathcal{Y} = \mathcal{Q} \cup \{?\}$, and a channel mapping $\texttt{adv} : \mathcal{X}^n \to \mathcal{Y}^n$ that is chosen from a set of mappings $\mathcal{ADV}$ by an *adversary* who seeks to disrupt communication between Alice and Bob. For each mapping $\texttt{adv} \in \mathcal{ADV}$, the channel constraint requires that the number of erasure symbols '?' and the number of symbol errors in the channel output cannot exceed rn and pn, respectively. The adversary chooses $\texttt{adv} \in \mathcal{ADV}$ using knowledge of Alice's message m, and adv not revealed to either Alice or Bob.

C. Codes with Feedback

For a rate $R \in (0,1]$, blocklength $n \geq 1$, and number of feedback bits $B \geq 0$, an (n, Rn, B)-code (with feedback) is a tuple $\Psi = (\mathcal{C}_k, \phi, f_k, \mathcal{T}, \mathcal{Z})$ that specifies the following communication scheme. First, the code Ψ specifies how Bob sends feedback to Alice. For an integer $T \geq 0$, Bob sends feedback in T rounds, sending a symbol from the feedback alphabet $\mathcal{Z}$ at each time in the set $\mathcal{T} = \{t_1,\ldots,t_T\}$ where $1 \leq t_1 < t_2 < \cdots < t_T < n$. For $k \in [T]$, the feedback symbol sent at time t_k is determined by the feedback function $f_k : \mathcal{Y}^{t_k} \to \mathcal{Z}$ and is denoted as $z_k = f_k(y_1,\ldots,y_{t_k})$ where $(y_1,\ldots,y_{t_k}) \in \mathcal{Y}^{t_k}$ is Bob's received sequence up to time t_k. Notice that B bits of feedback implies that $T\log_2|\mathcal{Z}| \leq B$.

Second, Ψ specifies how Alice communicates with Bob. For $k \in [T+1]$, Alice sends symbols in blocks of symbol size $t_k - t_{k-1}$ (where we define $t_0 = 0$ and $t_{T+1} = n$) using the encoding function $\mathcal{C}_k : \mathcal{M} \times \mathcal{Z}^{k-1} \to \mathcal{X}^{t_k - t_{k-1}}$. We denote Alice's transmitted symbols over this block as $(x_{t_{k-1}+1},\ldots,x_{t_k}) = \mathcal{C}_k(m; z_1,\ldots,z_{k-1})$. Finally, Alice decodes with the the decoding function $\phi : \mathcal{Y}^n \to \mathcal{M}$. We assume that adversary knows the code Ψ used by Alice and Bob and can use this knowledge to choose $\texttt{adv} \in \mathcal{ADV}$.

Let the symbol $\circ$ denote a concatenation between two sequences, i.e., $\boldsymbol{a}\circ\boldsymbol{b} = (\boldsymbol{a},\boldsymbol{b})$. We let $f(\boldsymbol{y})$ denote the concatenation $f_1(y_1,\ldots,y_{t_1}) \circ f_2(y_1,\ldots,y_{t_2}) \circ \cdots \circ f_T(y_1,\ldots,y_{t_T})$ and we let $\mathcal{C}(m; z_1,\ldots,z_T)$ denote the concatenation $\mathcal{C}_1(m) \circ \mathcal{C}_2(m,z_1) \circ \cdots \circ \mathcal{C}_{T+1}(m; z_1,\ldots,z_T)$. In the sequel, for any message $m \in \mathcal{M}$ and feedback sequence $(z_1,\ldots,z_T) \in \mathcal{Z}^T$ we refer to $\mathcal{C}(m; z_1,\ldots,z_T)$ as the *codeword* corresponding to m and $(z_1,\ldots,z_T)$. Similarly, for $k \in [T+1]$ we refer to $\mathcal{C}_k(m; z_1,\ldots,z_{k-1})$ as the *k-th sub-codeword* corresponding to m and $(z_1,\ldots,z_{k-1})$.

D. Capacity

A rate $R \in (0,1]$ is *(zero-error) achievable with $O(1)$-bit feedback under an error fraction p and erasure fraction r* if there exists a constant $B \geq 0$ and for all n large enough there exists an (n, Rn, B)-code $\Psi = (\mathcal{C}_k, \phi, f_k, \mathcal{T}, \mathcal{Z})$ such

that $\phi\left(\texttt{adv}(\mathcal{C}(m;\boldsymbol{z}))\right) = m$ for all $m \in \mathcal{M}$ and for all $\texttt{adv} \in \mathcal{ADV}$ where $\boldsymbol{z} = f(\texttt{adv}(\mathcal{C}(m;\boldsymbol{z})))$. The zero-error capacity $C_q(p,r)$ is the supremum of rates achievable with $O(1)$-bit feedback under an error fraction p and erasure fraction r.

III. Proof of Theorem 1: Upper Bound

We first present a summary of our proof followed by a detailed proof. In the sequel, we adopt the following setup. Let $q \geq 2$. Let $p \in [0, \frac{q-1}{2q}]$ and $r \in [0, \frac{q-1}{q}]$ be the fraction of symbol errors and erasures, respectively, where $2p + r \leq \frac{q-1}{q}$. The proof can be easily extended to account for the complement of this set. For $\bar{p} \in [0,p]$, let $\alpha(\bar{p}) = 1 - \frac{2q}{q-1}(p-\bar{p}) - \frac{q}{q-1}r$. Define $C_0 = \min_{\bar{p}\in[0,p]}[\alpha(\bar{p})\left(1 - H_q\left(\frac{\bar{p}}{\alpha(\bar{p})}\right)\right)]$.

A. Overview of Converse Proof

Roughly, the aim of our proof is to show that for any $\epsilon_R > 0$, rate $R = C_0 + \epsilon_R$ and any communication scheme using $O(1)$-bit feedback, there exists an adversarial strategy $\texttt{adv} \in \mathcal{ADV}$ and a message $m \in \mathcal{M}$ such that Bob incorrectly decodes m when sent by Alice. To be more precise, we define the notation of a *confusable* message pair.

For an (n, Rn, B)-code $\Psi = (\mathcal{C}_k, \phi, f_k, \mathcal{T}, \mathcal{Z})$, the pair of (unique) messages $m_1, m_2 \in \mathcal{M}$ is said to be confusable if there exists an adversarial channel mapping $\texttt{adv}^* \in \mathcal{ADV}$ such that the codewords corresponding to both messages m_1 and m_2 are mapped to the same received sequence $\boldsymbol{y}^* \in \mathcal{Y}^n$, i.e., $\boldsymbol{y}^* = \texttt{adv}^*(\mathcal{C}(m_1; z_1^*, \ldots, z_T^*)) = \texttt{adv}^*(\mathcal{C}(m_2; z_1^*, \ldots, z_T^*))$ for the feedback sequence $(z_1^*, \ldots, z_T^*) = f(\boldsymbol{y}^*)$. Thus, if some pair (m_1, m_2) is confusable, for any decoder ϕ used by Bob, the adversary can induce a decoding error for some message $m \in \{m_1, m_2\}$. Hence, for any $\epsilon_R > 0$ sufficiently small, $R = C_0 + \epsilon_R$, any integer constant $B \geq 1$ and for any (n, Rn, B)-code $\Psi = (\mathcal{C}_k, \phi, f_k, \mathcal{T}, \mathcal{Z})$, we show that for large enough n there exists a message pair (m_1, m_2) that is confusable. To show the existence of this pair, we provide a construction of $\texttt{adv}^*$ via the "babble-and-push" attack.

B. Summary of "Babble-and-Push" Attack

"Babble" Attack: Let m denote Alice's transmitted message which is drawn uniformly from $\mathcal{M}$ and known to the adversary and let $\bar{p} = \arg\min_{\bar{p}\in[0,p]}[\alpha(\bar{p})\left(1 - H_q\left(\frac{\bar{p}}{\alpha(\bar{p})}\right)\right)]$. For the first $b = (\alpha(\bar{p}) + \epsilon_R/2)n$ channel uses, the adversary randomly injects $\bar{p}n$ symbol errors into Alice's codeword. More specifically, the adversary randomly chooses a subset $\mathcal{S} \subset \{1, \ldots, b\}$ of size $\bar{p}n$, and subsequently chooses Bob's i^{th} received symbol y_i uniformly from $\mathcal{Q} \setminus \{x_i\}$ for all $i \in \mathcal{S}$ and sets $y_i = x_i$ for all $i \in [b] \setminus \mathcal{S}$. Let $\boldsymbol{x}_{\text{b}} = (x_1, \ldots, x_b)$ and $\boldsymbol{y}_{\text{b}} = (y_1, \ldots, y_b)$ denote Alice's transmitted codeword and Bob's received sequence up to time b, respectively, following the adversary's "babble" attack. Furthermore, let $T_{\text{b}} \in [0, T]$ denote the number of rounds of feedback that occur up to time b and let $z_1, \ldots, z_{T_{\text{b}}}$ denote the feedback symbols sent during these T_{b} rounds where $z_{T_{\text{b}}}$ is sent at time b.[7]

"Push" Setup: Following the "babble" attack, the adversary first constructs a set of all messages m' such that the first b symbols of sub-codeword $\mathcal{C}(m'; z_1, \ldots, z_T)$ are close to $\boldsymbol{y}_{\text{b}}$. That is, the adversary constructs the set $\mathcal{B}_{\boldsymbol{y}_{\text{b}}} = \left\{m' \in \mathcal{M} : d_H\left(\boldsymbol{y}_{\text{b}}, \mathcal{C}^{(\text{b})}(m'; z_1, \ldots, z_{T_{\text{b}}-1})\right) = \bar{p}n\right\}$ where $\mathcal{C}^{(\text{b})}(m'; z_1, \ldots, z_{T_{\text{b}}-1}) \triangleq \mathcal{C}_1(m') \circ \ldots \circ \mathcal{C}_{T_{\text{b}}}(m'; z_1, \ldots, z_{T_{\text{b}}-1})$ denotes the first b symbols of the codeword $\mathcal{C}(m'; z_1, \ldots, z_T)$.

Next, for each sub-codeword index $k \in \{T_{\text{b}} + 1, \ldots, T + 1\}$ and each feedback sequence $\boldsymbol{z}'_{k-1}$ that agrees with the feedback sent in the first b channel uses, i.e., $\boldsymbol{z}'_{k-1} \in \mathcal{Z}'_{k-1} \triangleq \{z_1\} \times \ldots \times \{z_{T_{\text{b}}}\} \times \mathcal{Z}^{k-1-T_{\text{b}}}$, the adversary constructs a set of all message pairs $(m', m'') \in \mathcal{B}^2_{\boldsymbol{y}_{\text{b}}}$ such that the k^{th} sub-codewords corresponding to m, $\boldsymbol{z}'_{k-1}$ and m', $\boldsymbol{z}'_{k-1}$ are close. Specifically, the adversary constructs the set $\mathcal{D}_{k,\boldsymbol{z}'_{k-1}} = \{(m', m'') \in \mathcal{B}^2_{\boldsymbol{y}_{\text{b}}} : m' \neq m'', d_H\left(\mathcal{C}_k(m'; \boldsymbol{z}'_{k-1}), \mathcal{C}_k(m''; \boldsymbol{z}'_{k-1})\right) \leq \Delta_k\}$ for some distance parameter $\Delta_k > 0$ and where we recall that $\mathcal{C}_k(m'; \boldsymbol{z}'_{k-1})$ is the k^{th} sub-codeword corresponding to m' and $\boldsymbol{z}'_{k-1}$. Subsequently, the adversary constructs the set of all strongly confusable message pairs $\mathsf{SCM}_{\boldsymbol{y}_{\text{b}}} = \bigcap_{k=T_{\text{b}}+1}^{T+1} \bigcap_{\boldsymbol{z}'_{k-1} \in \mathcal{Z}'_{k-1}} \mathcal{D}_{k,\boldsymbol{z}'_{k-1}}$.

By careful choice of Δ_k,[8] we have that for any pair $(m', m'') \in \mathsf{SCM}_{\boldsymbol{y}_{\text{b}}}$ and any feedback sequence $\boldsymbol{z}'_T \in \mathcal{Z}'_T$, the codewords corresponding to $m', \boldsymbol{z}'_T$ and $m'', \boldsymbol{z}'_T$ are close such that $d_H\left(\mathcal{C}^{(\text{p})}(m'; \boldsymbol{z}'_T), \mathcal{C}^{(\text{p})}(m''; \boldsymbol{z}'_T)\right) < 2(p-\bar{p})n + rn - \frac{n\epsilon_R}{16} \triangleq \Delta$ where $C^{(\text{p})}(m'; \boldsymbol{z}'_T)$ denotes the last $n - b$ symbols of the codeword $\mathcal{C}(m'; \boldsymbol{z}'_T)$. In Corollary 3.1, we show the existence of a received sequence $\boldsymbol{y}^*_{\text{b}} \in \mathcal{Y}^b$ and a message pair $(m_1, m_2) \in \mathsf{SCM}_{\boldsymbol{y}^*_{\text{b}}}$. In turn, we show that there exists a received sequence $\boldsymbol{y}^*_{\text{p}} \in \mathcal{Y}^{n-b}$ that a) has at most rn erasure symbols and b) is *close* to the codeword suffix corresponding to message m_i for $i = 1, 2$, i.e., $d_H(\mathcal{C}^{(\text{p})}(m_i; z_1^*, \ldots, z_{T_{\text{b}}}^*), \boldsymbol{y}^*_{\text{p}}) \leq (p - \bar{p})n - \frac{n\epsilon_R}{16}$ where $(z_1^*, \ldots, z_T^*) = f((\boldsymbol{y}^*_{\text{b}}, \boldsymbol{y}^*_{\text{p}}))$.

"Push" Attack: Let $\boldsymbol{x}_{\text{p}} = (x_{b+1}, \ldots, x_n)$ and $\boldsymbol{y}_{\text{p}} = (y_{b+1}, \ldots, y_n)$ denote Alice's transmission and Bob's received sequence, respectively, during the "push" attack. The adversary's push attack is as follows. If either $\boldsymbol{y}_{\text{b}} \neq \boldsymbol{y}^*_{\text{b}}$ or $m \notin \{m_1, m_2\}$, then the adversary takes no further action and $\boldsymbol{y}_{\text{p}} = \boldsymbol{x}_{\text{p}}$. Otherwise, if $\boldsymbol{y}_{\text{b}} = \boldsymbol{y}^*_{\text{b}}$ and $m \in \{m_1, m_2\}$, then the adversary chooses $\texttt{adv}$ to be the mapping which outputs $\boldsymbol{y}_{\text{p}} = \boldsymbol{y}^*_{\text{p}}$ (call this mapping $\texttt{adv}^*$). In summary, when Alice sends the message m_i for $i = 1, 2$, then with positive probability over the "babble" attack, $(\boldsymbol{y}^*_{\text{b}}, \boldsymbol{y}^*_{\text{p}}) = \texttt{adv}^*(\mathcal{C}(m; z_1^*, \ldots, z_T^*))$ where $(z_1^*, \ldots, z_T^*) = f((\boldsymbol{y}^*_{\text{b}}, \boldsymbol{y}^*_{\text{p}}))$.

[7] In our analysis and W.L.O.G., we consider a stronger communication scheme than initially described in the channel model. We strengthen the scheme by incrementing Bob's feedback budget by an additional bit and requiring Bob to send the extra bit of feedback immediately after channel use b. Thus, for any $(n, Rn, B+1)$-code used by Alice and Bob, we ensure that the T_{b}^{th} feedback symbol $z_{T_{\text{b}}}$ is sent immediately after the b^{th} channel use (i.e., at the end of the "babble" attack). The purpose of this assumption is to ensure that the adversary's "push" attack does not begin in the middle of a sub-codeword, thus simplifying our analysis of the "push" attack.

[8] Let $\beta_k \in (0, 1]$ be the ratio of the number of symbols in sub-codeword $\mathcal{C}_k$ and the number of remaining symbols $n - b$ after the "babble" attack, and set $\Delta_k = \begin{cases} 2(p-\bar{p})\beta_k n + r\beta_k n - \frac{\epsilon_R \beta_k n}{8}, & \beta_k \geq \frac{\epsilon_R}{16T} \\ (n-b)\beta_k, & \beta_k < \frac{\epsilon_R}{16T}. \end{cases}$

C. Analysis of "Babble-and-Push" Attack

Let M, $\boldsymbol{X}_{\mathrm{b}}$ and $\boldsymbol{Y}_{\mathrm{b}}$ denote the random variables corresponding to Alice's message, Alice's first b transmitted codeword symbols, and Bob's first b received symbols, respectively. Assume that M is uniformly distributed in the message set $\mathcal{M} = [q^{Rn}]$. Let $\mathcal{F} = \{\boldsymbol{Y}_{\mathrm{b}} \in \{\boldsymbol{y}_{\mathrm{b}} \in \mathcal{Y}^b : H(M|\boldsymbol{Y}_{\mathrm{b}} = \boldsymbol{y}_{\mathrm{b}}) \geq \frac{n\epsilon_R}{4}\}\}$ be the event that Bob still has uncertainty in message M after observing $\boldsymbol{Y}_{\mathrm{b}}$.

Lemma 1 ([15, Claim A.2])**.** $\mathbb{P}(\mathcal{F}) > \frac{\epsilon_R}{4}$.

Corollary 1.1. *Conditioned on event $\mathcal{F}$, the number of messages in $\mathcal{B}_{\boldsymbol{y}_{\mathrm{b}}}$ is at least $q^{\frac{n\epsilon_R}{4}}$.*

Lemma 2 (Plotkin Bound [23])**.** *A q-ary $(n, k, 0)$-code $\Psi = (\mathcal{C}, \phi)$ with minimum distance $d_{min} > (1 - 1/q)n$ must have a bounded number of codewords such that $|\mathcal{C}| \triangleq q^k \leq \frac{qd_{min}}{qd_{min} - (q-1)n}$.*

Lemma 3. *Conditioned on event $\mathcal{F}$, the set of strongly confusable messages $\mathsf{SCM}_{\boldsymbol{y}_{\mathrm{b}}}$ is non-empty for large enough n.*

Proof of Lemma 3. Recall that the set of all feedback sequences that Bob may send in the "push" phase which are consistent with the feedback $z_1, \ldots, z_{T_{\mathrm{b}}}$ sent during the "babble" phase is $\cup_{k=T_{\mathrm{b}}+1}^{T+1} \mathcal{Z}'_{k-1}$. Let I denote the number of sequences in this set, and in turn, let $\boldsymbol{z}^{(1)}, \boldsymbol{z}^{(2)}, \ldots, \boldsymbol{z}^{(I)}$ be any enumeration of sequences in this set. Note that for $i \in [I]$, we have that $\boldsymbol{z}^{(i)} \in \mathcal{Z}'_{k_i - 1}$ for some sub-codeword index $k_i \in [T_{\mathrm{b}} + 1, T + 1]$.

For each $i \in [I]$, we construct a graph to study the distance between a particular subset of all k_i^{th} sub-codewords corresponding to feedback sequence $\boldsymbol{z}^{(i)}$. For $i = 1, 2, \ldots, I$, consider a simple undirected graph $\mathcal{G}_i = (\mathcal{V}_i, \mathcal{E}_i)$ with a vertex set $\mathcal{V}_i$ consisting of some subset of sub-codewords $\{\mathcal{C}_{k_i}(m'; \boldsymbol{z}^{(i)}) : m' \in \mathcal{B}_{\boldsymbol{y}_{\mathrm{b}}}\}$ (we provide a detailed construction of $\mathcal{V}_i$ shortly). Two distinct sub-codewords $\boldsymbol{x}'$ and $\boldsymbol{x}''$ in $\mathcal{V}_i$ are connected by an edge if and only if $d_H(\boldsymbol{x}', \boldsymbol{x}'') \leq \Delta_{k_i}$.

To describe the construction of $\mathcal{V}_i$, we first define a maximum clique and a maximum independent set of $\mathcal{G}_i$. A *maximum clique* $\mathcal{K}_i$ of graph $\mathcal{G}_i$ corresponds to a largest subset of sub-codewords in $\mathcal{V}_i$ such that every 2 sub-codewords are within Hamming distance Δ_{k_i}. We let $\mathcal{K}_i$ be some maximum clique in case two or more such cliques may exists. A *maximum independent set* $\mathcal{I}_i$ of graph $\mathcal{G}_i$ corresponds to a largest subset of sub-codewords in $\mathcal{V}_i$ such that every 2 sub-codewords are not within Hamming distance Δ_{k_i}. Recall that Plotkin's bound (Lemma 2) provides an upper bound on the number of (sub-) codewords that are not within Hamming distance Δ_{k_i} from each other. In particular, the size of a maximum independent set is bounded such that $|\mathcal{I}_i| \leq \frac{q\Delta_{k_i}}{q\Delta_{k_i} - (q-1)(n-b)\beta_{k_i}}$. In turn, by substituting our above choice of Δ_{k_i}, the bound on $|\mathcal{I}_i|$ can be simplified to $|\mathcal{I}_i| \leq N \triangleq \max\{\frac{8(p-\bar{p})+8r}{3\epsilon_R}, q\}$ where we note that N is constant in n.

We now construct the vertex sets $\mathcal{V}_1, \mathcal{V}_2, \ldots, \mathcal{V}_I$ in a recursive manner such that the sub-codewords in $\mathcal{V}_i$ correspond to the messages of sub-codewords in the maximum clique $\mathcal{K}_{i-1}$. As the base case ($i = 1$), we define $\mathcal{V}_1 = \{\mathcal{C}_{k_1}(m'; \boldsymbol{z}^{(1)}) : m' \in \mathcal{B}_{\boldsymbol{y}_{\mathrm{b}}}\}$. For $i = 2, 3, \ldots, I$, the vertex set $\mathcal{V}_i = \{\mathcal{C}_{k_i}(m'; \boldsymbol{z}^{(i)}) : m' \in \mathcal{K}_{i-1}\}$ where $m' \in \mathcal{K}_{i-1}$ denotes the message m' corresponding to the sub-codeword $\mathcal{C}_{k_{i-1}}(m'; \boldsymbol{z}^{(i-1)}) \in \mathcal{K}_{i-1}$. Thus, all messages corresponding to sub-codewords in $\mathcal{V}_i$ have sub-codewords in $\mathcal{V}_{i-1}$ that are pairwise close. By construction, we have that if two unique messages m' and m'' have corresponding sub-codewords in $\mathcal{V}_I$, then m' and m'' have corresponding sub-codewords in $\mathcal{V}_i$ for *all* $i \in \{1, \ldots, I\}$ and, in turn, $(m', m'') \in \mathsf{SCM}_{\boldsymbol{y}_{\mathrm{b}}}$. Thus, to prove Lemma 3, it is sufficient to show that the vertex set $\mathcal{V}_I$ contains at least two sub-codewords. This is equivalent to showing that maximum clique $\mathcal{K}_{I-1}$ contains at least two sub-codewords.

We show the above sufficient condition by lower bounding the size of clique $\mathcal{K}_i$. We introduce the *Ramsey number* $\mathrm{R}(|\mathcal{K}|, |\mathcal{I}|)$ which is the smallest integer such that every simple undirected graph of size $\mathrm{R}(|\mathcal{K}|, |\mathcal{I}|)$ has a clique of size $|\mathcal{K}|$ or an independent set of size $|\mathcal{I}|$. Recall that the size of the maximum independent set $\mathcal{I}_i$ is at most N. Thus, for $K \geq 1$, if the size of the vertex set $\mathcal{V}_i$ is at least $\mathrm{R}(K, N + 1)$, then the size of the maximum clique $\mathcal{K}_i$ is at least K.

We now prove by induction that for large enough n, the size of $\mathcal{K}_i$ is at least $L_i(q^n)$ for $i = 1, \ldots, I - 1$ where $L_i(q^n)$ denotes the composition $\log_q \circ \log_q \circ \cdots \circ \log_q(q^n)$ of i number of logarithms. (*Base Case*) Suppose that event $\mathcal{F}$ occurs. Then by Corollary 1.1, the size of $\mathcal{V}_1$ is at least $q^{\frac{n\epsilon_R}{4}}$. It follows that the size of $\mathcal{K}_1$ is at least $L_1(q^n) = n$ if $\mathrm{R}(n, N + 1) \leq q^{\frac{n\epsilon_R}{4}}$. Indeed, for large enough n

$$\mathrm{R}(n, N + 1) \overset{(a)}{\leq} \tbinom{n+N-1}{N} \overset{(b)}{\leq} 2^{(n+N-1)H_2\left(\frac{N}{n+N-1}\right)} \overset{(c)}{\leq} q^{\frac{n\epsilon_R}{4}}$$

where (a) follows from the bound that for any $|\mathcal{K}|, |\mathcal{I}| \geq 1$, $\mathrm{R}(|\mathcal{K}|, |\mathcal{I}|)$ is at most $\binom{|\mathcal{I}|+|\mathcal{K}|-2}{|\mathcal{I}|-1}$ [24], (b) follows from the bound $\binom{n}{k} \leq 2^{nH_2(k/n)}$ for $k \leq n/2$, and (c) follows for large enough n from the fact that N constant in n. Thus, $|\mathcal{K}_1| \geq n$. Base case done. (*Induction*) Let $i \in \{2, \ldots, I-2\}$ and assume that the size of $\mathcal{K}_{i-1}$ is at least $L_{i-1}(q^n)$. Following the construction of $\mathcal{V}_i$, the size of $\mathcal{V}_i$ is equal to the size of $\mathcal{K}_{i-1}$. Similar to the argument made in the base case, we have that $|\mathcal{K}_i| \geq L_i(q^n)$ if $\mathrm{R}(L_i(q^n), N + 1) \leq |\mathcal{V}_i| \triangleq |\mathcal{K}_{i-1}|$. Indeed, for large enough n, $\mathrm{R}(L_i(q^n), N + 1) \leq \binom{L_i(q^n)+N-1}{N}$ $\leq L_{i-1}(q^n) \leq |\mathcal{K}_{i-1}| \triangleq |\mathcal{V}_i|$ where the bound $L_{i-1}(q^n) \leq |\mathcal{K}_{i-1}|$ follows from assumption. In conclusion, for large enough n, $|\mathcal{K}_i| \geq L_i(q^n)$ for all $i \in [I - 1]$. Since the number of feedback bits $B + 1$ is a constant in n, it follows that I is a constant and, in turn, $L_{I-1}(q^n) \geq 2$ for large enough n. Thus, for large enough n, $\mathcal{K}_{I-1}$ contains at least two sub-codewords. ∎

Let blocklength n be large enough such that Lemma 3 holds. Let $\boldsymbol{y}_{\mathrm{b}}^* \in \mathcal{Y}^b$ be any received sequence such that $\boldsymbol{Y}_{\mathrm{b}} = \boldsymbol{y}_{\mathrm{b}}^*$ with positive probability and $H(M|\boldsymbol{Y}_{\mathrm{b}} = \boldsymbol{y}_{\mathrm{b}}^*) \geq \frac{n\epsilon_R}{n}$. To complete the proof, we note the following corollary of Lemma 3.

Corollary 3.1. *With positive probability over the "babble" attack and choice of Alice's message, $\boldsymbol{Y}_{\mathrm{b}} = \boldsymbol{y}_{\mathrm{b}}^*$ and there exists messages m_1 and m_2 such that $(m_1, m_2) \in \mathsf{SCM}_{\boldsymbol{y}_{\mathrm{b}}^*}$.*

REFERENCES

[1] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[2] E. Berlekamp, "On the number of correctable errors for transmission over a binary symmetrical channel with feedback," PhD dissertation, Massachusetts Institute of Technology, 1964.

[3] K. Zigangirov, "On the number of correctable errors for transmission over a binary symmetrical channel with feedback," *Probl. Peredachi Inf.*, vol. 12, no. 2, pp. 3–19, 1976.

[4] R. Ahlswede, C. Deppe, and V. Lebedev, "Non–binary error correcting codes with noiseless feedback, localized errors, or both," in *Proc. IEEE Int. Symp. Inf. Theory*, July 9 - 14, 2006.

[5] B. Haeupler, P. Kamath, and A. Velingker, "Communication with partial noiseless feedback," in *APPROX/RANDOM 2015*, ser. Leibniz International Proc. in Informatics (LIPIcs), vol. 40, 2015, pp. 881–897.

[6] P. Joshi, A. Purkayastha, Y. Zhang, A. Budkuley, and S. Jaggi, "On the capacity of additive AVCs with feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, June 26 - July 1, 2022.

[7] M. Gupta, V. Guruswami, and R. Y. Zhang, "Binary error-correcting codes with minimal noiseless feedback," arXiv:2212.05673, 2022.

[8] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inf. Theory*, vol. 6, no. 4, pp. 445–450, 1990.

[9] D. J. Love, R. W. Heath, V. K. N. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE J. Sel. Areas. Commun.*, vol. 26, no. 8, 2008.

[10] E. N. Gilbert, "A comparison of signaling alphabets," *Bell Syst. Tech. J.*, vol. 31, no. 3, p. 504–522, 1952.

[11] R. Varshamov, "Estimate of the number of signals in error correcting codes," *Dokl. Acad. Nauk*, vol. 117, pp. 739–741, 1957.

[12] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte—MacWilliams inequalities," *IEEE Trans. Inf. Theory*, vol. 23, no. 2, pp. 157 – 166, 1977.

[13] B. K. Dey, S. Jaggi, M. Langberg, and A. D. Sarwate, "Upper bounds on the capacity of binary channels with causal adversaries," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3753 – 3763, 2013.

[14] C. Chen, S. Jaggi, and M. Langberg, "A characterization of the capacity of online (causal) binary channels," in *Proc. ACM STOC*, 15-17 June 2014, pp. 287–296.

[15] Z. Chen, S. Jaggi, and M. Langberg, "The capacity of online (causal) q-ary error-erasure channels," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3384–3411, 2019.

[16] M. A. Tsfasman, S. G. Vladut, and T. Zink, "Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound," *Math. Nachrichten*, vol. 109, no. 1, pp. 21–28, 1982.

[17] A. D. Sarwate, "Coding against myopic adversaries," in *Proc. 2010 IEEE Inf. Theory Workshop*, 2010.

[18] B. K. Dey, S. Jaggi, and M. Langberg, "Sufficiently myopic adversaries are blind," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5718 – 5736, 2019.

[19] E. Ruzomberka, C.-C. Wang, and D. J. Love, "Channel capacity for adversaries with computationally bounded observations," in *Proc. IEEE Int. Symp. Inf. Theory*, June 26 - July 1 2022.

[20] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Tran. Inf. Theory*, vol. 34, no. 2, 1988.

[21] V. Suresh, E. Ruzomberka, C.-C. Wang, and D. Love, "Causal adversarial channels with feedback snooping," *IEEE J. Sel. Topics Inf. Theory*, vol. 3, no. 1, pp. 69–84, 2022.

[22] Y. Zhang, S. Jaggi, M. Langberg, and A. D. Sarwate, "The capacity of causal adversarial channels," arXiv:2205.06708, 2022.

[23] I. Blake and R. Mullin, *An Introduction to Algebraic and Combinatorial Coding Theory*. Academic Press, 1976.

[24] R. E. Greenwood and A. M. Gleason, "Combinatorial relations and chromatic graphs," *Canadian J. Math.*, vol. 17, pp. 1–7, 1955.