Improved Upper Bounds on the Capacity of Binary Channels with Causal Adversaries

Bikash Kumar Dey
IIT Bombay
bikash@ee.iitb.ac.in

Sidharth Jaggi
CUHK
jaggi@ie.cuhk.edu.hk

Michael Langberg
The Open University of Israel
mikel@openu.ac.il

Anand D. Sarwate
TTI-Chicago
asarwate@ttic.edu

***Abstract*—In this work we consider the communication of information in the presence of a *causal* adversarial jammer. In the setting under study, a sender wishes to communicate a message to a receiver by transmitting a codeword $\mathbf{x} = (x_1, \ldots, x_n)$ bit-by-bit over a communication channel. The adversarial jammer can view the transmitted bits x_i one at a time, and can change up to a p-fraction of them. However, the decisions of the jammer must be made in a *causal* manner. Namely, for each bit x_i the jammer's decision on whether to corrupt it or not (and on how to change it) must depend only on x_j for $j \leq i$. This is in contrast to the "classical" adversarial jammer which may base its decisions on its complete knowledge of $\mathbf{x}$. Binary channels with causal adversarial jammers have seen recent studies in which both lower bounds and upper bounds on their capacity is derived. In this work, we present improved upper bounds on the capacity which hold for both deterministic and stochastic encoding schemes.**

I. Introduction

Alice wishes to transmit a message u to Bob over a binary-input binary-output channel. To do so, she encodes u into a length-n binary vector $\mathbf{x}$ and transmits it over the channel. However, the channel is controlled by a malicious adversary Calvin who may observe the transmissions, and attempts to jam communication by flipping up to a fraction p of the bits Alice transmitted. Since he must act in a causal manner, Calvin's decisions on whether or not to flip bit x_i must be a function solely of the bits $x_1, \ldots, x_i$ he has observed thus far. This communication scenario models jamming by an adversary who is limited in his jamming capability (perhaps due to limited processing power or limited transmit energy) and is causal. This *causality* assumption is reasonable for many communication channels, both wired and wireless, where Calvin is not co-located with Alice. Calvin can only corrupt a bit when it is transmitted (and thus its error is based on its view so far). To decode the transmitted message, Bob waits until all the bits have arrived.

Our main contribution in this work is an *impossibility result* that helps make progress towards a better understanding of the communication rates achievable against a causal adversary. Specifically, we describe and analyze a particular jamming strategy of Calvin, and show that it (upper) bounds the rate of communication no matter what coding strategy Alice and Bob use. The jamming strategy, corresponding analysis and resulting bound are all novel.

Authors are in alphabetical order. Work supported in part by ISF grant 480/08, RGC GRF grants 412608 and 412809, RGC AoE grant on Institute of Network Coding, established under the University Grant Committee of Hong Kong, CUHK MoE-Microsoft Key Laboratory of Humancentric Computing and Interface Technologies, the Bharti Centre for Communication in IIT Bombay, India, and the California Institute for Telecommunications and Information Technology (CALIT2) at UC San Diego.

A. Previous and related work

Many of the following works deal with more general channels; we mostly restrict our discussion to the binary-input binary-output case.

Coding theory model: A very strong class of adversarial channels is one where Calvin is *omniscient* – he knows Alice's entire codeword $\mathbf{x}$ prior to transmission and can tailor the pattern of up to pn bit-flips to each specific transmission. This is the worst-case noise model studied in coding theory. For binary channels, characterizing the capacity using deterministic codes has been an open problem for several decades. The best known upper bound is due to McEliece *et al.* [1] as the solution of an LP, and the best known achievable scheme corresponds to codes suggested by Gilbert and Varshamov [2], [3], which achieve a rate of $1 - H(2p)$. Improving either of these bounds would be a significant breakthrough.

Information theory model: A much weaker class of adversarial channels is one where Calvin generates coin flips in an i.i.d. manner. The original work of Shannon [4] effectively characterized the capacity of such channels.

Causal adversarial model: The class of channels considered in this work, *i.e.*, that of *causal adversaries*, fall in between these two extremes. In one direction this is because a causal adversary is certainly no stronger than an omniscient adversary, since he cannot tailor his jamming strategy to take into account Alice's future transmissions. Indeed, the work of [5] indicates that (for $p < H^{-1}(1/2) \simeq 0.055$) rates strictly better than those achievable by GV codes against an omniscient adversary are achievable against a causal adversary. However, since it is still unknown whether GV codes are optimal against omniscient adversaries, it is unknown whether causal adversaries are indeed strictly weaker than omniscient adversaries. In the other direction, prior work [6] demonstrates definitively that a causal adversary is *strictly* "stronger" than random noise – in particular, for all p such that $H(p) < 4p$ (i.e., $p > 0.0157$), the best rates achievable against a causal adversary are strictly bounded away from the rate of $1 - H(p)$ achievable against a random BSC(p). The results in [6] hold for deterministic coding schemes, and leave the possibility of

stochastic codes in most open. In stochastic codes, Alice may encode u to one of several possible codewords $\mathbf{x} \in \{\mathbf{x}(u,r)\}$), where r is a random source available to Alice but unknown to either Bob or Calvin. Stochastic codes can in some scenarios achieve rates greater than achievable via deterministic codes.

In this work, our contribution is two fold. We present *strictly* tighter upper bounds than those presenting in [6], and in addition we show that our upper bounds hold for both deterministic and stochastic encoding.

Arbitrarily Varying Channels: The information-theoretic arbitrarily varying channel (AVC) model captures the notion of causality [7], however research on causal adversaries has been left open [7], [8]. AVC models have been extended to include channels with constraints on the adversary (such as pn bit flips) for cases where the adversary has no access to the codeword [9], or has access to the full codeword [10].

Delayed adversaries: A refinement of the causal adversary model, called the *delayed adversary*, was studied in [11] and [12]. In these models, the jammer's decision on whether to corrupt x_i must depend only on x_j for $j \leq i - dn$ for a delay parameter $d \in [0,1]$. The case of $d = 0$ is exactly the standard causal setting, and that of $d = 1$ corresponds to the "oblivious adversary" studied in [11]. The authors [12] showed that for a large class of channels, the capacity for delay $d > 0$ equals that of the information-theoretic AVC model.

The works most relevant to ours are those stated above and the works [13], [14] which address computational aspects of coding.

B. Main result

Our improved bounds are given in the following theorem, and are depicted (in comparison with the previous bounds) in Figure 1. As mentioned above, our bounds improve over previous ones and hold for both stochastic codes. Let $p \in [0,1/4]$. Consider any $\bar{p} \in [0,p]$. Let $\alpha(p,\bar{p}) = 1-4(p-\bar{p})$. In what follows, $C(p)$ is the capacity of the causal channel under study. For precise definitions and model see Section II.

Theorem 1. $C(p) \leq \min_{\bar{p}\in[0,p]} \left[\alpha(p,\bar{p})\left(1 - H\left(\frac{\bar{p}}{\alpha(p,\bar{p})}\right)\right)\right]$.

It can be shown that the optimum $\bar{p}$ is approximately $\min\{p,(1-4p)/8.4445\}$. Namely, for $p > 0.0804$, the capacity $C(p)$ is bounded away from $1-H(p)$ and for $p < 0.0804$ our bound equals $1-H(p)$.

C. Techniques and Proof Overview

To prove Theorem 1 we must present a strategy for Calvin that does not allow communication at rate higher than $C(p)$ (no matter which encoding/decoding scheme is used by Alice and Bob). Specifically, the strategy we present will allow Calvin to enforce a constant probability of error bounded away from zero whenever Alice and Bob communicate at rate higher than $C(p)$. Roughly speaking, Calvin uses a two-phase *babble-and-push* strategy. In the first phase of $\ell(p)$ channel uses, Calvin "babbles" by behaving like a BSC($\bar{p}$) for some $\bar{p}$ chosen as a function of p. In the second phase of $n-\ell(p)$ channel uses, Calvin randomly selects a codeword from Alice and Bob's codebook which is consistent with what Bob has received so far. Calvin then "pushes" the remaining part of Alice's codeword towards his selected codeword.

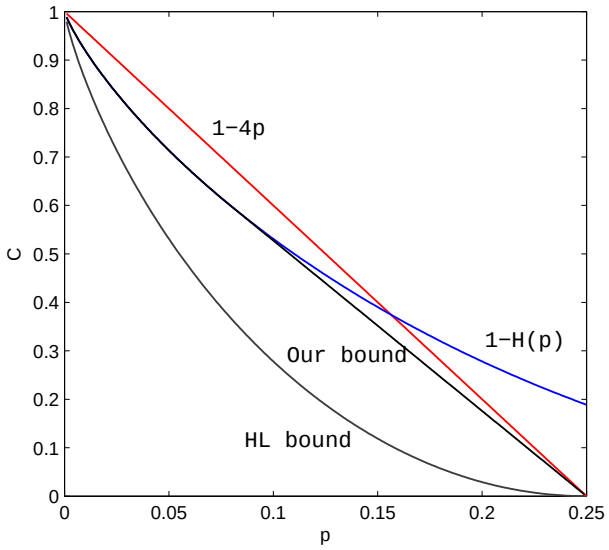

Figure 1. We plot all previous bounds related to the channel at hand compared to our new bound. The *upper* bound of [6] is $\min(1-4p, 1-H(p))$ for $p \in [0,1/4]$ and 0 for $p > 1/4$ and is represented by the blue and red lines. The *lower* bound of [5] (denoted HL) is represented by the black line. Our improved bound appears in between.

II. Model

For any positive integer k, let $[k] = \{1,2,\ldots,k\}$. We let $\mathcal{U} = [2^{nR}]$ denote Alice's message set, and $\mathbf{U}$ denote the message random variable uniformly distributed in $\mathcal{U}$. A *deterministic code* of rate R and blocklength n is a pair of maps $\mathcal{C}_d = (\Phi, \Psi)$ where $\Phi : \mathcal{U} \to \mathcal{X}^n$ and $\Psi : \mathcal{Y}^n \to \mathcal{U}$ are a deterministic maps. The map Φ is called the encoder and the map Ψ is called the decoder.

A *code with stochastic encoding* of rate R and blocklength n is a pair of maps $\mathcal{C}_s = (\Phi, \Psi)$ where $\Phi : \mathcal{U} \to \mathcal{X}^n$ is a random map and $\Psi : \mathcal{Y}^n \to \mathcal{U}$ is a deterministic map. The random map Φ gives a probability distribution $\rho(\cdot|u)$ on $\mathcal{X}^n$ for every $u \in \mathcal{U}$. Such an encoding is equivalently represented by first picking a random variable $\mathfrak{R}$ from a set $\mathscr{R}$ (with $|\mathscr{R}| \leq |\mathcal{X}|^n$) according to a conditional distribution $\rho_{\mathfrak{R}|\mathbf{U}}(.|u)$, and then using a deterministic encoder map $\Phi : \mathcal{U} \times \mathscr{R} \to \mathcal{X}^n$. Note that our definition does not preclude there existing pairs (u,r) and (u',r') such that $\Phi(u,r) = \Phi(u',r')$.

A *causal adversarial strategy* of blocklength n is a sequence of random maps $\mathsf{Adv} = \{f_{\mathcal{C}}^{(i)} : i \in [n]\}$ where $f_{\mathcal{C}}^{(i)} : \mathcal{X}^i \to \mathcal{E}$ takes a code (deterministic or with stochastic encoding) $\mathcal{C}$ and for each channel use $i \in [n]$ uses the past and current inputs $(x_1, x_2, \ldots, x_i)$ to choose an action $e_i = f_{\mathcal{C}}^{(i)}(x_1,\ldots,x_i) \in \mathcal{E}$ at time i, with resulting output $y_i = x_i + e_i$. The strategy obeys constraint p if $\sum_{i=1}^n e_i \leq pn$ almost surely over the randomness in the message, encoder, and strategy. For a given adversarial strategy and an input codeword $\mathbf{x}$, the strategy

produces a (possibly random) $\mathbf{e}$ and the output is $\mathbf{y} = \mathbf{x} \oplus \mathbf{e}$. Let $\mathbb{P}_{\mathsf{Adv}}(\mathbf{y}|\mathbf{x})$ denote the probability of an output $\mathbf{y}$ given an input $\mathbf{x}$ under the strategy Adv. When the blocklength is understood from the context, let $\mathsf{Adv}(p)$ denote all adversarial strategies obeying constraint p.

The (average) probability of error for a code with stochastic encoding is given by

$$\bar{\varepsilon}_s = \max_{\mathsf{Adv}\in\mathsf{Adv}(p)} \frac{1}{2^{Rn}} \sum_{u=1}^{2^{Rn}} \sum_{r\in\mathscr{R}} \rho(\Phi(u,r)|u) \sum_{\mathbf{y}} \mathbb{P}_{\mathsf{Adv}}(\mathbf{y}|\Phi(u,r))\mathbf{1}\left(\Psi(\mathbf{y}) \neq u\right) \quad (1)$$

We can interpret the errors as the error in expectation over Alice choosing a message $\mathbf{U} = u$ and a codeword $\mathbf{x} = \Phi(u,r)$ according to the conditional distribution $\rho(\mathbf{x}|u)$.

A rate R is *achievable* against a causal adversary under average error if for every $\delta > 0$ there exist infinitely many block lengths $\{n_i\}$, such that for each n_i there is an n_i block length code (with stochastic encoding) of rate at least R and average probability of error at most δ. The supremum of all achievable rates is the capacity. We denote by $C(p)$ the capacity of the channel corresponding to adversaries parametrized by p.

Consider a code of blocklength n, rate R and error probability δ. We can, without loss of generality (wlog), assume that the encoding probabilities $\{\rho(\mathbf{x}|u) : \mathbf{x} \in \{0,1\}^n, u \in [2^{nR}]\}$ are rational. To see why this is the case, note that for any small $\eta > 0$ we can find rational numbers $\{\tilde{\rho}(\mathbf{x}|u)\}$ such that $\rho(\mathbf{x}|u) - \eta \leq \tilde{\rho}(\mathbf{x}|u) \leq \rho(\mathbf{x}|u)$. Now consider a code with encoding probabilities $q(\mathbf{x}|u) = \tilde{\rho}(\mathbf{x}|u)$ for $\mathbf{x} \neq \mathbf{0}$ and assign the remaining probability to $\mathbf{0}$. Under the same decoder, this code has error probability at most $\delta + 2^{n+nR}\eta$, but since η was arbitrary, the error is at most 2δ.

Now, for a given stochastic code, let N be the least common multiple of the denominators of $\rho(\mathbf{x}|u)$ for all $\mathbf{x}, u$. We can imagine each codeword $\mathbf{x}$ of u as $N\rho(\mathbf{x}|u)$ copies of the same codeword with conditional probability $1/N$ each. So we can equivalently associate a random variable $\mathfrak{R}$ with $|\mathscr{R}| = N$ s.t. the conditional distribution $\rho_{\mathfrak{R}|\mathbf{U}}(\cdot|u)$ is uniform, and the encoding map $\Phi(u,\cdot)$ is not necessarily one-one. Since we consider uniform message distribution, henceforth, wlog, we assume that the joint distribution $\rho_{\mathfrak{R},\mathbf{U}}(\cdot,\cdot)$ is uniform.

III. Proof of Theorem 1

Let $p \in [0, 1/4]$ and let $\bar{p} \leq p$. Let $\varepsilon > 0$. In what follows we prove that the rate of communication over the causal adversarial channel (with parameter p) is bounded by $R = C + \varepsilon$ where $C = \left[\alpha(p,\bar{p})\left(1 - H\left(\frac{\bar{p}}{\alpha(p,\bar{p})}\right)\right)\right]$ and $\alpha(p,\bar{p}) = 1 - 4(p-\bar{p})$ as defined in Theorem 1. Namely, for any sufficiently large block length n, and any (n-block stochastic) code $\mathcal{C}_s = (\Phi, \Psi)$ shared by Alice and Bob, there exists an adversarial jammer Adv that can impose a constant decoding error. The decoding error we will obtain will depend on $\varepsilon > 0$.

The proof for $p = \bar{p}$ follows from previous works as described in the Introduction. Thus, we assume that $p - \bar{p} > 0$ and that $\varepsilon < 2(p - \bar{p})$. In what follows, we fix a block length n (which will at times be assumed to be sufficiently large with respect to $1/\varepsilon$).

Adversarial strategy: Our converse bound is based on a particular two-phase adversarial strategy for Calvin that we call "babble-and-push." Let $\ell = (\alpha + \varepsilon/2)n$ and without loss of generality assume $\ell \in \mathbb{N}$. For a vector $\mathbf{z}$ of length n, let $\mathbf{z}_1 = (z_1, z_2, \ldots, z_\ell)$ and $\mathbf{z}_2 = (z_{\ell+1}, z_{\ell+2}, \ldots, z_n)$.

- **(Babble)** Calvin chooses a random subset Γ of $\bar{p}n$ indices uniformly from all $(\bar{p}n)$-subsets of $\{1, 2, \ldots, \ell\}$. For $i \in \Gamma$, Calvin flips bit x_i; that is, for $i \in \{1, 2, \ldots, \ell\}$, $e_i = 1$ for $i \in \Gamma$ and $e_i = 0$ for $i \notin \Gamma$.
- **(Push)** Calvin constructs the set of (u,r) that are *confusable* with $\mathbf{y}_1$. Namely, Calvin constructs the set

$$B_{\mathbf{y}_1} = \{(u,r) : d_H(\mathbf{y}_1 - \Phi(u,r)) = \bar{p}n\}, \quad (2)$$

and selects an element $(u',r') \in B_{\mathbf{y}_1}$ uniformly at random. Calvin then picks the corresponding codeword $\mathbf{x}' = \Phi(u',r')$. Given a selected $\mathbf{x}'$, for $i > \ell$, if $x_i \neq x'_i$, Calvin sets e_i equiprobably to 0 or 1 until $\sum_{j=1}^{i} e_j = pn$ or $i = n$. Note that, under our assumption (wlog) of uniform $\rho_{\mathbf{U},\mathfrak{R}}$, the *a posteriori* distribution of Alice's choice (u,r) given $\mathbf{y}_1$ is also uniform in $B_{\mathbf{y}_1}$.

Analysis: We start by proving the following technical lemma that we use in our proof.

Lemma 2. *Let V be a random variable on a discrete finite set $\mathcal{V}$ with entropy $H(V) > \lambda$, and let $V_1, V_2, \ldots, V_m$ be i.i.d. copies of V. Then*

$$\Pr\left[\{V_i : i = , \ldots, m\} \text{ are all distinct}\right] \geq \left(\frac{\lambda - m}{\log|\mathcal{V}|}\right)^{m-1} \quad (3)$$

Proof: Fix $i \leq m$ and a set $v_1, v_2, \ldots, v_i \in \mathcal{V}$. Let $A = \{v_1, \ldots, v_i\}$ and let $W = \mathbf{1}(V \in A)$. We can write the distribution of V as a mixture:

$$\Pr[V = v] = \sum_{j=0,1} \Pr[W = j] \cdot \Pr[V|W = j]$$

We can upper bound the entropy of V:

$$\begin{aligned} H(V) &\leq H(V|W) + H(W) \\ &= \sum_{j=0,1} \Pr[W = j] H(V|W = j) + H(W) \end{aligned}$$

Since conditioning reduces entropy and the support of V conditioned on W is at most i, we have

$$\lambda \leq 1 + \log i + \Pr[W = 0] \log|\mathcal{V}|.$$

Namely, $Pr[W = 0] \geq \frac{\lambda - 1 + \log i}{\log|\mathcal{V}|}$. Thus a loose bound on the desired event is $(\frac{\lambda - m}{\log|\mathcal{V}|})^{m-1}$. ∎

To prove the upper bound, we now present a series of claims.

Claim 3. *With probability at least $\varepsilon/2$ over the adversarial strategy of Calvin, the realization $\mathbf{y}_1$ of the output satisfies*

$$H(\mathbf{U}|\mathbf{Y}_1 = \mathbf{y}_1) \geq n\varepsilon/4, \quad (4)$$

where the entropy is measured over the randomness of the encoder.

Proof: By the data processing inequality, and the choice of Calvin's strategy, we have

$$\begin{aligned} I(\mathbf{U};\mathbf{Y}_1) &\le I(\mathbf{X}_1;\mathbf{Y}_1) \\ &\le \ell(1-H(\bar{p}n/\ell)) \\ &\le (\alpha n+\varepsilon n/2)\left(1-H\left(\frac{\bar{p}}{\alpha+\varepsilon/2}\right)\right) \end{aligned}$$

Therefore

$$\begin{aligned} H(\mathbf{U}|\mathbf{Y}_1) &\ge H(\mathbf{U}) - n(\alpha+\varepsilon/2)\left(1-H\left(\frac{\bar{p}}{\alpha+\varepsilon/2}\right)\right) \\ &\ge n\left(\varepsilon+\alpha\left(1-H\left(\frac{\bar{p}}{\alpha}\right)\right)\right) \\ &\qquad - n(\alpha+\varepsilon/2)\left(1-H\left(\frac{\bar{p}}{\alpha+\varepsilon/2}\right)\right) \\ &> n\varepsilon/2. \end{aligned}$$

Thus the expected value of $H(\mathbf{U}|\mathbf{Y}_1=\mathbf{y}_1)$ over $\mathbf{y}_1$ is at least $n\varepsilon/2$. The maximum value of $H(\mathbf{U}|\mathbf{Y}_1=\mathbf{y}_1)$ is nR, so with probability at least $\varepsilon/2$, we have $H(\mathbf{U}|\mathbf{Y}_1=\mathbf{y}_1)\ge n\varepsilon/4$ (via Markov inequality). ■

Now consider drawing m pairs (V_i,S_i) from $B_{\mathbf{y}_1}$ i.i.d. $\sim \rho_{\mathbf{U},\mathfrak{R}|\mathbf{y}_1}$ (which happens to be uniform). The marginal distribution of V_i is also i.i.d. $\sim \rho_{\mathbf{U}|\mathbf{y}_1}$, which is not necessarily uniform.

Claim 4. *Let $\rho_{\mathbf{U}|\mathbf{y}_1}$ be the conditional distribution of $\mathbf{U}$ given $\mathbf{y}_1$ under the adversarial strategy of Calvin. Let $V_1,V_2,\ldots,V_m$ be m random variables drawn i.i.d. according to $\rho_{\mathbf{U}|\mathbf{y}_1}$. Then conditioned on Claim 3, for any $m\ge 1$ there is an n sufficiently large such that the event*

$$E_1 = \{\text{the elements } \{V_i\}_{i=1}^m \text{ are all distinct}\},$$

has probability bounded from below: $\Pr[E_1]\ge(\varepsilon/8)^{m-1}$.

Proof: The proof follows from Claim 3 and Lemma 2 by using $\lambda=n\varepsilon/4$ and the fact that there are at most 2^n messages. The bound then becomes $(\varepsilon/4-m/n)^{m-1}$. For fixed m there exists an n sufficiently large so that $m/n\le\varepsilon/8$. ■

Conditioning on values of $\mathbf{y}_1$ that satisfy Claim 3, and using the fact that Alice's pair (u,r) is random in $B_{\mathbf{y}_1}$, we now analyze the probability that Calvin chooses a pair (u',r') in $B_{\mathbf{y}_1}$ such that (a) $u\ne u'$ and (b) $d_H(\mathbf{x}_2(u,r),\mathbf{x}_2'(u',r'))<2(p-\bar{p})n-\varepsilon n/8$. These two events will allow Calvin to succeed in the remaining "push" phase of his corruption.

Claim 5. *Conditioned on Claim 3, with probability at least $\varepsilon^{O(1/\varepsilon)}$, both (a) and (b) above hold.*

Proof: Let $\mathbf{y}_1$ satisfy Claim 3, so that $H(\rho_{U|\mathbf{y}_1})\ge\varepsilon n/4$. Let γ be the fraction of couples (u,r) and (u',r') in $B_{\mathbf{y}_1}$ that satisfy (a) and (b) above.

First consider randomly sampling $\{(u_i,r_i):i\in[m]\}$ uniformly from $B_{\mathbf{y}_1}$, and let $\mathbf{x}^i$ be the codeword for (u_i,r_i). Claim 4 shows that the messages $\{u_i\}$ are distinct with probability $(\varepsilon/8)^{m-1}$.

Now consider the event

$$E_2=\{\exists\mathbf{x},\mathbf{x}'\in\{\mathbf{x}^i\}_{i=1}^m:\ d_H(\mathbf{x}_2,\mathbf{x}_2')<2(p-\bar{p})n-\varepsilon n/8\}.$$

By Plotkin's bound [15] there do not exist binary error correcting codes of minimum distance greater than or equal to d with more than $\frac{2d}{2d-(4(p-\bar{p})n-\varepsilon n/2)}+1$ codewords. Thus for $m=17/\varepsilon$, applying this bound with $d=2(p-\bar{p})n-\varepsilon n/8$ to the set $\{\mathbf{x}_2^i\}$ shows that there must exist two codewords close to each other, so $\Pr[E_2|E_1]=1$. Here E_1 is the event specified in Claim 4.

Now let $E_3(\mathbf{x},\mathbf{x}')$ be the event that $d_H(\mathbf{x}_2,\mathbf{x}_2')<2(p-\bar{p})n-\varepsilon n/8$ and $u\ne u'$, so $Pr[E_3(\mathbf{x}^i,\mathbf{x}^j)]=\gamma$. Then:

$$\Pr\left[\bigcup_{\mathbf{x},\mathbf{x}'\in\{\mathbf{x}^i\}_{i=1}^m}E_3(\mathbf{x},\mathbf{x}')\right]\le m^2\gamma.$$

But

$$\begin{aligned} \Pr\left[\bigcup_{\mathbf{x},\mathbf{x}'\in\{\mathbf{x}^i\}_{i=1}^m}E_3(\mathbf{x},\mathbf{x}')\right] &\ge \Pr[E_1\cap E_2] \\ &= \Pr[E_2|E_1]\Pr[E_1] \\ &\ge (\varepsilon/8)^{m-1}. \end{aligned}$$

Thus

$$\gamma\ge\frac{1}{m^2}\left(\frac{\varepsilon}{8}\right)^{m-1}=\frac{17^2}{\varepsilon^2}\left(\frac{\varepsilon}{8}\right)^{17/\varepsilon-1}.$$

Therefore with probability at least γ, (a) and (b) hold. ■

The next step is to show that Calvin does not "run out" of bit flips during the second "push" phase of his attack. This follows directly from Sanov's Theorem [16].

Claim 6. *Conditioned on Claim 5, with probability at least* $1-2^{-\Omega(\varepsilon^2 n)}$

$$d_H(\mathbf{x},\mathbf{y})\in\left(\left(\frac{d}{2}+\bar{p}n\right)-\frac{\varepsilon n}{16},\left(\frac{d}{2}+\bar{p}n\right)+\frac{\varepsilon n}{16}\right). \quad (5)$$

Claim 7. *For any code with stochastic encoding of rate $R=C+\varepsilon$, under Calvin's babble-and-push strategy the average error probability $\bar{\varepsilon}_2$ is lower bounded by $\varepsilon^{O(1/\varepsilon)}$* **Anand's remark**: Check statement to see if it matches etc

Proof: The main result of the converse is that conditioned on Claim 3, Claim 5, and Claim 6, Calvin can "symmetrize" the channel [9]. Let (u,r) denote the message and randomness of Alice, $\mathbf{y}_1$ be the received codeword in the babble phase, and (u',r') be the message and randomness chosen by Calvin for the push phase. Let $\rho(\mathbf{y}_1,u,r,u',r')$ be the joint distribution of these variables under Alice's uniform choice of (u,r) and Calvin's attack. For each $\mathbf{y}$, let $\rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r')$ be the conditional distribution of $\mathbf{y}$ under Calvin's attack.

The error probability can be written as

$$\bar{\varepsilon}_s = \sum_{\mathbf{y}_1,u,r,u',r'} \rho(\mathbf{y}_1,u,r,u',r') \sum_{\mathbf{y}_2} \rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r')\mathbf{1}(\Psi(\mathbf{y}) \neq u)$$

Let $\mathcal{F}$ be the set of tuples $(\mathbf{y}_1,u,r,u',r')$ satisfying Claim 3 and Claim 5. These claims show that $\rho(\mathcal{F}^c) \geq (\varepsilon/2)\cdot\varepsilon^{O(1/\varepsilon)}$. For $(\mathbf{y}_1,u,r,u',r') \in \mathcal{F}$, we have that $u \neq u'$, and $\mathbf{x}_2(u,r)$ and $\mathbf{x}_2(u',r')$ are sufficiently close.

Let $\mathcal{G}$ be the set of $\mathbf{y}_2$ such that Claim 6 is satisfied for $\mathbf{x}_2(u,r)$. Note that by the symmetry of Calvin's attack in the push phase, for $(\mathbf{y}_1,u,r,u',r') \in \mathcal{F}$, Claim 6 is also satisfied for $\mathbf{x}_2(u',r')$. Indeed, for $\mathbf{y}_2 \in \mathcal{G}$, the conditional distribution is symmetric:

$$\rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r') = \rho(\mathbf{y}|\mathbf{y}_1,u',r',u,r) \tag{6}$$

Then for $(\mathbf{y}_1,u,r,u',r') \in \mathcal{F}$, by Claim 6,

$$\begin{aligned}\sum_{\mathbf{y}:\Psi(\mathbf{y})\neq u} \rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r') + \sum_{\mathbf{y}:\Psi(\mathbf{y})\neq u'} \rho(\mathbf{y}|\mathbf{y}_1,u',r',u,r) &\geq \sum_{\mathbf{y}_2\in\mathcal{G}} \rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r') \\ &\geq 1 - 2^{-\Omega(\varepsilon^2 n)}.\end{aligned}$$

Now, returning to the overall error probability, let $\rho(\mathbf{y}_1)$ be the unconditional probability of Bob receiving $\mathbf{y}_1$ in the babble phase, where the probability is taken over Alice's uniform choice of (u,r) and Calvin's random babble $\mathbf{e}_1$. We rewrite the joint distribution as

$$\begin{aligned}\rho(\mathbf{y}_1,u,r,u',r') &= \sum_{\mathbf{y}_1}\rho(\mathbf{y}_1) \sum_{(u,r)\in B_{\mathbf{y}_1}} \sum_{(u',r')\in B_{\mathbf{y}_1}} \frac{1}{|B_{\mathbf{y}_1}|^2} \\ &= \sum_{\mathbf{y}_1}\rho(\mathbf{y}_1) \sum_{(u',r')\in B_{\mathbf{y}_1}} \sum_{(u,r)\in B_{\mathbf{y}_1}} \frac{1}{|B_{\mathbf{y}_1}|^2}.\end{aligned}$$

Thus

$$\begin{aligned}2\bar{\varepsilon}_s &\geq \sum_{\mathcal{F}} \rho(\mathbf{y}_1,u,r,u',r') \\ &\left(\sum_{\mathbf{y}:\Psi(\mathbf{y})\neq u} \rho(\mathbf{y}|\mathbf{y}_1,u,r,u',r') + \sum_{\mathbf{y}:\Psi(\mathbf{y})\neq u'} \rho(\mathbf{y}|\mathbf{y}_1,u',r',u,r)\right) \\ &\geq \varepsilon/2\cdot\varepsilon^{O(1/\varepsilon)}\cdot\left(1-2^{-\Omega(\varepsilon^2 n)}\right)\end{aligned}$$

■

Thus a decoding error happens if the conditions of Claim 3, Claim 5, Claim 6, and Claim 7 are all satisfied. **Anand's remark**: *check this still:* This implies a refined statement of Theorem 1. Namely, let c be a sufficiently large constant. For any block length n, any $\varepsilon > 0$ and any encoding/decoding scheme of Alice and Bob of rate $\left(C(p)+\sqrt{\frac{c}{n}}\right)+\varepsilon$, Calvin can cause a decoding error of at least $\Omega\left(\varepsilon^2+\frac{1}{n}\right)$. ■

IV. Concluding remarks

In this work we present a novel upper bound on the rates achievable against a causal adversary, which strictly improves on prior upper bounds known against such adversaries over binary channels. Further, we demonstrate that the upper bound presented herein holds against arbitrary codes, rather than simply against deterministic codes, as is common in the coding theory literature. Since our analysis pertains to adversarial jamming rather than random noise, the proof techniques presented may be of independent interest in the more general setting of AVC's.

References

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

[2] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Systems Technical Journal*, vol. 31, pp. 504–522, 1952.

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

[4] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423,623–656, July, October 1948.

[5] H. Ishay and M. Langberg, "Beating the Gilbert-Varshamov bound for online channels," *Proceedings of the 2011 International Symposium on Information Theory*, pp. 1297–1301, 2011.

[6] M. Langberg, S. Jaggi, and B. Dey, "Binary causal-adversary channels," in *Proceedings of the 2009 International Symposium on Information Theory (ISIT)*, 2009.

[7] D. Blackwell, L. Breiman, and A. Thomasian, "The capacities of certain channel classes under random coding," *Annals of Mathematical Statistics*, vol. 31, pp. 558–567, 1960.

[8] I. Csiszár and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems, 2nd edition*. New York, NY: Akademiai Kiado, 1997.

[9] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited : Positivity, constraints," *IEEE Transactions on Information Theory*, vol. 34, no. 2, pp. 181–193, 1988.

[10] A. D. Sarwate and M. Gastpar, "Rateless codes for AVC models," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3105–3114, July 2010. [Online]. Available: http://dx.doi.org/10.1109/TIT.2010.2048497

[11] M. Langberg, "Oblivious channels and their capacity," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 424–429, 2008.

[12] M. Langberg, S. Jaggi, and B. Dey, "Coding against delayed adversaries," in *Proceedings of the 2010 International Symposium on Information Theory (ISIT)*, 2010.

[13] A. Smith, "Scrambling adversarial errors using few random bits, optimal information reconciliation, and better private codes," in *Proceedings of the 2007 ACM-SIAM Symposium on Discrete Algorithms (SODA 2007)*, 2007.

[14] V. Guruswami and A. Smith, "Explicit capacity-achieving codes for worst-case additive errors," arXiv:0912.0965v1 [cs.IT].

[15] A. E. Brouwer, "Bounds on the size of linear codes," *Handbook of Coding Theory, Elsevier Science, New York, NY, USA*, vol. 1, pp. 295–461, 1998.

[16] T. M. Cover and J. A. Thomas, *Elements of information theory, 2nd edition*. New York, NY, USA: Wiley-Interscience, 2006.