Authenticated partial correction over AV-MACs: toward characterization and coding

Duncan Koepke, Michaela Schnell, Madelyn St.Pierre, Allison Beemer

Department of Mathematics, University of Wisconsin-Eau Claire

Eau Claire, WI, United States

Abstract—In this paper we study γ partial correction over a t-user arbitrarily varying multiple-access channel (AV-MAC). We first present necessary channel conditions for the γ partially correcting authentication capacity region to have nonempty interior. We then give a block length extension scheme which preserves positive rate tuples from a short code with zero probability of γ partial correction error, noting that the flexibility of γ partial correction prevents pure codeword concatenation from being successful. Finally, we offer a case study of a particular AV-MAC satisfying the necessary conditions for partial correction.

Index Terms—arbitrarily varying multiple-access channel, capacity region, authentication, partial correction

I. Introduction

An arbitrarily varying multiple-access channel (AV-MAC) combines random noise with adversarial action over a channel with multiple senders and a single receiver. Classical communication over AV-MACs has been studied in a variety of works, with [1]–[4] focusing on the capacity region in the two-user case. The combination of these works establish the communication capacity region, notably showing that the region has nonempty interior if and only if the channel does not have a set of channel *symmetrizability* properties. Symmetrizability, defined for point-to-point AVCs in [5], indicates that the adversary can reliably trick the receiver into decoding in error.

While symmetrizability characterizes the communication capacity of an AVC, the analogous condition of *overwritability* governs the (keyless) *authentication* capacity of such a channel [6]. Overwritability indicates that an adversary is not only able to trick the receiver into an erroneous message estimate, but that they are able to do so *while remaining undetected*. In [7], Beemer et al. formalize an extension of overwritability to the AV-MAC, in a similar vein to the extension of symmetrizability for communication. They show that the capacity region for (keyless) authentication over an AV-MAC is equal to that for communication with no adversary, provided that the channel is not overwritable to any degree.

Other work related to authentication over an AV-MAC includes work on MACs with byzantine users. In [8], [9], Sangwan et al. consider a byzantine user in a two-user MAC, proving results on the authenticated communication capacity region. Indeed, the inner bound of the authentication capacity region for two users over an AV-MAC in [7] was accomplished

by fixing the byzantine user in an an extension to three users of the scheme of [8]. In general, however, the question of a byzantine user in a MAC is distinct from an AV-MAC, where the adversary's identity is known a priori.

In the present work, we give the extensions of authentication results from [7] to the case of an arbitrary number of users, then quickly turn our attention the idea of γ *partial correction*. Partial correction over an AV-MAC was introduced in [7] to bridge the gap between total correction and authentication. In contrast to pure authentication, γ partial correction requires that a γ fraction of users' messages be decoded correctly, even if the remainder be discarded. The particular users who are decoded accurately may change with each transmission: that is, the subset of users to be decoded is not fixed ahead of time. When $\gamma = 0$, this reduces to authentication, while with $\gamma = 1$ the goal becomes classical communication.

To our knowledge, partial correction over an AV-MAC has only been studied in [7]. However, we note that there may be a connection to list decoding over AV-MACs (see e.g. [10], [11]), wherein partial correction would require that elements in the output list match on a certain number of users. In [7], the authors focus on the two-user case, and give some initial results showing that it is possible for a channel to have a γ partially correcting authentication capacity region with nonempty interior. Here, we extend these results to an arbitrary number of users. We give a set of necessary symmetrizability/overwritability conditions for γ partial correction, present a case study for a particular channel satisfying these conditions, and provide a scheme to extend block length that preserves positive rate tuples.

Necessary background and notation is introduced in Section II. In Section III, we present a set of necessary channel conditions for partial correction capacity regions with nonempty interior. Section IV discusses a general method for extending the block length of a short block length code tuple with desirable partial correction properties, and Section V provides a case study of the construction of these short codes for a particular channel. Section VI concludes the paper.

II. Preliminaries

Let $[n] := \{1, 2, \ldots, n\}$, and let $\text{supp}(\mathbf{x}) \subseteq [n]$ denote the support of a length-n vector $\mathbf{x}$. Capital letters (e.g. X) will denote random variables, script letters the alphabets they are taken from ($\mathcal{X}$), and lower case letters their realizations (x).

Our setting will be a t-user AV-MAC, where $t \geq 2$. More specifically, a t-user AV-MAC is defined by a distribution $W_{Y|X_1 \cdots X_t S}$, where legitimate channel inputs X_j are taken from alphabet $\mathcal{X}_j$ for each $j \in [t]$, the adversary's choice of channel *state* is $S \in \mathcal{S}$, and the channel output is given by $Y \in \mathcal{Y}$. In our model, we assume the adversary has full knowledge of the channel statistics and all user encoding strategies, but that S is independent of the particular message sequence transmitted in any given time instance. We begin by extending the definitions of [7].

Definition II.1. An $(M_1, \ldots, M_t, n)$ *authentication code* for a t-user AV-MAC is given by encoders $f_1, \ldots, f_t$ and decoder ϕ:

$$f_i : [M_j] \to \mathcal{X}_j^n, \ 1 \leq j \leq t \tag{1}$$
$$\phi : \mathcal{Y}^n \to ([M_1] \cup \{0\}) \times \cdots \times ([M_t] \cup \{0\}), \tag{2}$$

where an output of "0" in any coordinate indicates adversarial interference.

We will sometimes directly discuss the codebooks $C_j = f_j(M_j) \subseteq \mathcal{X}_j^n$ in later sections. In this paper, we will be concerned primarily with correcting some portion of the users' messages, even if others must be discarded due to adversarial interference.

Definition II.2. Let $\gamma \in (0,1)$. We say that an $(M_1, \ldots, M_t, n)$ authentication code for a t-user AV-MAC is γ *partially correcting* if, with high probability in n, we can correct at least $\lceil \gamma t \rceil$ of the t messages.

We observe that the case where $\gamma = 0$ reduces to the classical notion of authentication for an AV-MAC à la [7]–[9], while $\gamma = 1$ bridges the gap to total correction of all user messages. The use of the open interval in Definition II.2 excludes the cases where no messages are corrected, or all are; neither of these is *partial* correction. It is straightforward that if an authentication code is γ partially correcting, then it is λ partially correcting for all $0 < \lambda < \gamma$.

Let $\phi^{-1}(A) \subseteq \mathcal{Y}^n$ represent the set of channel outputs which decode to some element $(i_1, \ldots, i_t)$ in the set A under the decoder ϕ, and let $\phi^{-1}(A)^c$ be the complement in $\mathcal{Y}^n$ of this set. Let $\mathbf{x}_j(i) := f_j(i)$ denote the length-n encoding of message i by user j. Correspondingly, we let $\mathbf{i}$ denote a tuple of transmitted messages from $[M_1] \times \cdots \times [M_t]$, and $\mathbf{x}(\mathbf{i})$ its encoding under $(f_1, f_2, \ldots f_t)$. Given a tuple of transmitted messages, $\mathbf{i}$, and adversarial state $\mathbf{s}$, where $\mathbf{s} = \mathbf{s}_0$ denotes that the no-adversary state sequence, we define the *probability of γ partial correction error* for the authentication code $(f_1, \ldots, f_t, \phi)$ by:

$$e_\gamma(\mathbf{i}, \mathbf{s}_0) = W(\phi^{-1}(\{\mathbf{i}\})^c \mid \mathbf{x}(\mathbf{i}), \mathbf{s}_0), \tag{3}$$

and, when $\mathbf{s} \neq \mathbf{s}_0$,

$$e_\gamma(\mathbf{i}, \mathbf{s}) = W(\phi^{-1}(A_\mathbf{i})^c \mid \mathbf{x}(\mathbf{i}), \mathbf{s}), \tag{4}$$

where $A_\mathbf{i} = \{\hat{\mathbf{i}} : \hat{i}_j \in \{0, i_j\} \text{ for } j \in [t], |\text{supp}(\hat{\mathbf{i}})| \geq \lceil \gamma t \rceil \}$. That is, $A_\mathbf{i}$ is the set of decoded sequences that match sent

message tuple $\mathbf{i}$ on every nonzero entry, and have at least a γ fraction of nonzero entries. We will assume that each message in $[M_1] \times \cdots \times [M_t]$ is transmitted with equal probability, so that the average probability of error for a given adversarial choice of $\mathbf{s}$ is:

$$e_\gamma(\mathbf{s}) = \frac{1}{M_1 \cdots M_t} \sum_\mathbf{i} e_\gamma(\mathbf{i}, \mathbf{s}). \tag{5}$$

We say that a rate tuple $(R_1, \ldots, R_t) \in \mathbb{R}_{\geq 0}^t$ is *achievable for γ partial correction* if there exists a sequence of $(2^{R_1 n}, \ldots, 2^{R_t n}, n)$ codes such that $\max_\mathbf{s} e_\gamma(\mathbf{s})$ approaches 0 with increasing block length n. As in a point-to-point AVC or the two-user AV-MAC case, $\text{argmax}_\mathbf{s} e_\gamma(\mathbf{s})$ is the adversary's best chance of inducing a decoding error.

The (t-dimensional) *authentication capacity region* $\mathscr{C}_{\text{auth}}$ and the γ *partially correcting authentication capacity region*, $\mathscr{C}_{\text{auth}, \gamma}$, are the closures of the sets of achievable rate tuples for each respective goal, where the former is realized when $\gamma = 0$. Let $\mathscr{C}$ denote the communication capacity region in the no-adversary setting (i.e., $\mathbf{s} = \mathbf{s}_0$, $\gamma = 1$). We say that a capacity region has *nonempty interior* if it contains a point such that all coordinate values are positive.

Critical to authentication and partial correction are the concepts of *symmetrizability* [5] and *overwritability* [6]: channel conditions which determine whether a channel is amenable to these types of communication. Below, we give extensions to the original point-to-point definitions to a t-user AV-MAC:

Definition II.3. Let $t \geq 2$ and $m \in [t]$. A t-user AV-MAC $W_{Y|X_1 \cdots X_t S}$ (denoted by W) is $X_{i_1} \times \cdots \times X_{i_m}$-*symmetrizable* if there exists $P := P_{S|X_{i_1} \cdots X_{i_m}}$ such that for all $x_{i_1}, \ldots, x_{i_m}, x'_{i_1}, \ldots, x'_{i_m}, y$,

$$\sum_s P(s \mid x'_{i_1}, \ldots, x'_{i_m}) W(y|x_{i_1}, \ldots, x_{i_m}, s) =$$
$$\sum_s P(s \mid x_{i_1}, \ldots, x_{i_m}) W(y|x'_{i_1}, \ldots, x'_{i_m}, s).$$

The case $t = 2$ results in the symmetrizability conditions of [2], which along with [1], [3] showed that (lack of) symmetrizability completely characterizes when the AV-MAC communication capacity region $\mathscr{C}$ has (non)empty interior.

Definition II.4. Let $t \geq 2$ and $m \in [t]$. A t-user AV-MAC $W_{Y|X_1 \cdots X_t S}$ (denoted by W) is $X_{i_1} \times \cdots \times X_{i_m}$-*overwritable* if there exists $P := P_{S|X_{i_1} \cdots X_{i_m}}$ such that for all $x_{i_1}, \ldots, x_{i_m}, x'_{i_1}, \ldots, x'_{i_m}, y$,

$$\sum_s P(s \mid x'_{i_1}, \ldots, x'_{i_m}) W(y|x_{i_1}, \ldots, x_{i_m}, s) =$$
$$W(y|x'_{i_1}, \ldots, x'_{i_m}, s_0).$$

Again, the case of $t = 2$ reduces to previous results: it was shown in [7] that (lack of) overwritability completely characterizes when the authentication capacity region $\mathscr{C}_{\text{auth}}$ has (non)empty interior.

For brevity, we will say that a channel is m-*symmetrizable* (resp., -*overwritable*) if there exists some subset of m

users $i_1, \ldots, i_m$ such that the channel is $X_{i_1} \times \cdots \times X_{i_m}$-symmetrizable (resp., overwritable).

III. NECESSARY CONDITIONS FOR NONEMPTY INTERIOR

Previous work completely classified the authentication capacity region $\mathscr{C}_{\text{auth}}$ for the case of two users, and established necessary conditions for nonempty interior of the $\gamma = 0.5$ partially correcting authentication capacity region $\mathscr{C}_{\text{auth},0.5}$ in the same setting [7]. In this section, we extend these results to more than two users. Because the authentication rate region is not the primary topic of this paper, and the results extend in a straightforward way to more users, we omit the following proof pertaining to $\mathscr{C}_{\text{auth}}$; this result extends Lemma III.6 and Theorem III.7 of [7].

Theorem III.1. *A t-user AV-MAC is m-overwritable for some $m \in [t]$ if and only if $\mathscr{C}_{\text{auth}}$ has empty interior. Otherwise, $\mathscr{C}_{\text{auth}} = \mathscr{C}$.*

The following result on $\mathscr{C}_{\text{auth},\gamma}$ can be seen by observing that any γ partially correcting authentication code is simultaneously an authentication code. The result extends Lemma IV.2. of [7].

Lemma III.2. *For any t-user AV-MAC and $\gamma \in (0,1)$, $\mathscr{C}_{\text{auth},\gamma} \subseteq \mathscr{C}_{\text{auth}}$.*

Theorem III.1 and Lemma III.2 together imply that non-m-overwritability (for all $m \in [t]$) is a necessary condition for $\mathscr{C}_{\text{auth},\gamma}$ to have nonempty interior. Next, we give another necessary condition for nonempty interior of $\mathscr{C}_{\text{auth},\gamma}$. Namely, the channel can only be symmetrizable up to the number of users we need *not* correct to achieve γ partial correction. While this result extends Theorem IV.3 of [7], its proof contains more subtlety than the two-user case, so we include it here in full.

Theorem III.3. *Let $\gamma \in (0,1)$. If a t-user AV-MAC $W_{Y|X_1 \cdots X_t S}$ is m-symmetrizable for any $m > t - \lceil \gamma t \rceil$, then $\mathscr{C}_{\text{auth},\gamma}$ has empty interior.*

Proof. Let $\gamma \in (0,1)$. Suppose $W := W_{Y|X_1 \cdots X_t S}$ is $X_{i_1} \times \cdots \times X_{i_m}$-symmetrizable, where $m > t - \lceil \gamma t \rceil$. Without loss of generality, let $i_j = j$, so that the coordinates in question are the first m, and let $P := P_{S|X_1 \cdots X_m}$ be an adversarial distribution satisfying the property of Definition II.3. Consider a sequence of $(M_1, \ldots, M_t, n)$ codes, with $M_j := 2^{R_j n}$ where $R_j > 0$ for $j \in [t]$. Let $\mathbf{x}(\mathbf{i})$ be the encoding of message vector $\mathbf{i}$, and let $\mathbf{v}_a^b$ denote coordinates a through b of a vector $\mathbf{v}$. Define $A_{\mathbf{i}} := \{\hat{\mathbf{i}} : \hat{i}_j \in \{0, i_j\} \text{ for } j \in [t], |\text{supp}(\hat{\mathbf{i}})| \geq \lceil \gamma t \rceil\}$, as in Section II. Finally, define $M := (M_1 \cdots M_m)(M_1 \cdots M_t)$. Then, $\max_{\mathbf{s}} e_\gamma(\mathbf{s})$ is bounded below by the expected value of $e_\gamma(\mathbf{s})$ over S:

$$\geq \sum_{\mathbf{s}} \left(\frac{1}{M_1 \cdots M_m} \sum_{\mathbf{i}_1^m} P(\mathbf{s} \mid \mathbf{x}(\mathbf{i})_1^m) \right) e_\gamma(\mathbf{s}) \qquad (6)$$

$$= \frac{1}{M} \sum_{\mathbf{i}_1^m, \mathbf{k}, \mathbf{s}} P(\mathbf{s} \mid \mathbf{x}(\mathbf{i})_1^m) e_\gamma(\mathbf{k}, \mathbf{s}) \qquad (7)$$

$$\geq \frac{1}{M} \sum_{\mathbf{i}_1^m, \mathbf{k}, \mathbf{s}} P(\mathbf{s} \mid \mathbf{x}(\mathbf{i})_1^m) W(\phi^{-1}(A_{\mathbf{k}})^c \mid \mathbf{x}(\mathbf{k}), \mathbf{s}) \qquad (8)$$

$$= \frac{1}{M} \sum_{\mathbf{i}_1^m, \mathbf{k}, \mathbf{s}} P(\mathbf{s} \mid \mathbf{x}(\mathbf{k})_1^m) W(\phi^{-1}(A_{\mathbf{k}})^c \mid \mathbf{x}(\mathbf{i}_1^m \mathbf{k}_{m+1}^t), \mathbf{s}) \qquad (9)$$

where Equations (7) and (8) follow by definition, and (9) from symmetrizability.

Now, we consider the sets $A_{\mathbf{i}_1^m \mathbf{k}_{m+1}^t}$ and $A_{\mathbf{k}}$. If $i_j \neq k_j$ for all $j \in [m]$, then these two sets are disjoint: indeed, any decoded message tuple with support of size at least $\lceil \gamma t \rceil$ must contain at least one coordinate from the first m (recall that $m > t - \lceil \gamma t \rceil$). In other words, $\phi^{-1}(A_{\mathbf{i}_1^m \mathbf{k}_{m+1}^t}) \subseteq \phi^{-1}(A_{\mathbf{k}})^c$ when $i_j \neq k_j$ for all $j \in [m]$. Using that $R_j > 0$, and thus that the set of $\mathbf{i}_1^m$'s such that $i_j \neq k_j$ for fixed $\mathbf{k}$ is nonempty,

$$\geq \frac{1}{M} \sum_{\substack{\mathbf{k}, \mathbf{s} \\ \mathbf{i}_1^m : i_j \neq k_j}} P(\mathbf{s} \mid \mathbf{x}(\mathbf{k})_1^m) \cdot \qquad (10)$$

$$W(\phi^{-1}(A_{\mathbf{i}_1^m \mathbf{k}_{m+1}^t}) \mid \mathbf{x}(\mathbf{i}_1^m \mathbf{k}_{m+1}^t), \mathbf{s}) \qquad (11)$$

$$= \frac{1}{M} \sum_{\substack{\mathbf{k}, \mathbf{s} \\ \mathbf{i}_1^m : i_j \neq k_j}} P(\mathbf{s} \mid \mathbf{x}(\mathbf{k})_1^m) \left(1 - e_\gamma(\mathbf{i}_1^m \mathbf{k}_{m+1}^t, \mathbf{s})\right) \qquad (12)$$

$$= \frac{1}{M} \sum_{\mathbf{s}, \mathbf{k}_1^m} P(\mathbf{s} \mid \mathbf{x}(\mathbf{k})_1^m) \sum_{\substack{\mathbf{i}_1^m \mathbf{k}_{m+1}^t : \\ i_j \neq k_j}} \left(1 - e_\gamma(\mathbf{i}_1^m \mathbf{k}_{m+1}^t, \mathbf{s})\right) \qquad (13)$$

$$\geq \frac{1}{M} \sum_{\mathbf{s}, \mathbf{k}_1^m} P(\mathbf{s} \mid \mathbf{x}(\mathbf{k})_1^m) \left(\prod_{a=1}^{m}(M_a - 1) \prod_{b=m+1}^{t} M_b - e_\gamma(\mathbf{s}) \right) \qquad (14)$$

$$\geq \left(\frac{\prod_{a=1}^{m}(M_a - 1) \prod_{b=m+1}^{t} M_b}{M_1 \cdots M_t} - \max_{\mathbf{s}} e_\gamma(\mathbf{s}) \right) \frac{\sum_{\mathbf{k}_1^m} 1}{M_1 \cdots M_m} \qquad (15)$$

$$= \frac{\prod_{a=1}^{m}(M_a - 1) \prod_{b=m+1}^{t} M_b}{M_1 \cdots M_t} - \max_{\mathbf{s}} e_\gamma(\mathbf{s}) \qquad (16)$$

Altogether,

$$\max_{s} e_\gamma(\mathbf{s}) \geq \frac{\prod_{a=1}^{m}(M_a - 1) \prod_{b=m+1}^{t} M_b}{2 M_1 \cdots M_t}. \qquad (17)$$

The lower bound approaches 0.5 in n given that $R_j > 0$ for $j \in [m]$, bounding $\max_s e_\gamma(\mathbf{s})$ away from zero. We conclude that it is not possible that all R_j's, $j \in [m]$, were positive. Thus, $\mathscr{C}_{\text{auth},\gamma}$ has empty interior. $\qquad \square$

As in the two user case, it is possible that a channel is not overwritable in any sense, but is m-symmetrizable for some $m > t - \lceil \gamma t \rceil$; in this case, Theorem III.3 tells us that $\mathscr{C}_{\text{auth},\gamma}$ has empty interior, even while $\mathscr{C}_{\text{auth}} = \mathscr{C}$ may not. Furthermore, the proof of Theorem III.3 shows something slightly stronger than what is stated in the theorem: the projection of $\mathscr{C}_{\text{auth},\gamma}$ onto any m symmetrizable coordinates ($m > t - \lceil \gamma t \rceil$) must have empty interior.

IV. Block Length Extension Scheme

In this section, we present a method for extending the block length of a γ partially correcting authentication code whose probability of γ partial correction error is equal to zero. We note that unlike the classical ($\gamma = 1$) message correction case, simple concatenation of such a code will not automatically achieve the same rate as that of the original codebook: this is due to the fact that the particular $\lceil \gamma t \rceil$ users whose messages can be corrected in each time instance may vary. To adapt to our scenario, we use a concatenated code with the inner code tuple equal to a γ partially correcting code with probability of γ partial correction error equal to zero, and outer codes $C_{\varepsilon, j}$ given by a point-to-point codes designed for an induced erasure channel with a power constrained adversary. This induced channel is described in detail later in this section. A simplified version of this scheme appears in [7] for a particular two-user AV-MAC (a channel that is extended to more users in the case study of Section V). Here, we extend the scheme to the case of an arbitrary number of users. We note that our scheme is not channel-dependent beyond the assumption that such an inner code exists.

Suppose we have a set of t codebooks, each of block length n, that have correction capability $\gamma := \frac{u}{t}$ (with zero probability of γ partial correction error).[1] If each user concatenates r codewords from their codebook, at least u users are correctable in any given time instance, while the remainder will be deemed to be in erasure. Notice that at most $t - u$ users experience erasure in each of the r time instances. Our outer codes, $C_{\varepsilon, j}$, must protect against these erasures for at least u of the users. To gain an understanding of how this induced erasure channel functions, consider the following example:

Example IV.1. *Consider a set of three codebooks that have partial correction capability $\gamma = \frac{2}{3}$ and block length n, where $C_i := f_i(M_i) = \{c_{i1}, c_{i2}\}$ for $i \in [3]$. To extend the block length, we will use outer codes $C_{\varepsilon, j} \subseteq \mathbb{F}_2^6$. For example, let $C_{\varepsilon, j} = \{100101, 011101, 000101, 111010\}$ for all $j \in [3]$. Let 0 be replaced by the first codeword in each of the C_j's and 1 be replaced by the second codeword in each of the C_j's. For example the first codebook would become*

$$C_1' = \{c_{12}c_{11}c_{11}c_{12}c_{11}c_{12}, \ c_{11}c_{12}c_{12}c_{12}c_{11}c_{12},$$
$$c_{11}c_{11}c_{11}c_{12}c_{11}c_{12}, \ c_{12}c_{12}c_{12}c_{11}c_{12}c_{11}\}$$

with block length $6n$ and rate $\frac{2}{6n} = \frac{1}{3n}$. Because the C_j's can correct $\gamma t = 2$ of the three users, there will be a maximum of one erasure in each time instance. An example erasure pattern is given below, where an erasure is represented by ε. Note that with this erasure pattern, we can still correct two of the three users' messages, and thus achieve the goal of γ partial correction.

User 1	ε	ε	ε	ε	ε	ε
User 2	c_{22}	c_{21}	c_{21}	c_{22}	c_{21}	c_{22}
User 3	c_{31}	c_{32}	c_{32}	c_{32}	c_{31}	c_{31}

[1]For fixed t and integer $1 \leq u < t$, we take $\frac{u-1}{t} \leq \gamma < \frac{u}{t}$ and "round" it to $\frac{u}{t}$. This will not affect the number of users correctable due to the ceiling function on $\lceil \gamma t \rceil$.

The above erasure pattern example suggests that the adversary's best strategy will be to spread their efforts across enough users, but not any more than needed, in order to deter γ partial correction. Intuitively, the adversary should choose to target $t - u + 1$ users to have the most erasures per affected user while not leaving u users with zero erasures. The optimal strategy is formalized in the proof of the following lemma.

Lemma IV.2. *Let $t \geq 2$ and $1 \leq u < t$. If a $\gamma = \frac{u}{t}$ partially correcting codebook tuple (with error probability zero) is concatenated r times, at least u users will experience at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ total erasures.*

Proof. In each time instant, the adversary can attempt to erase $t - u$ users' symbols. If they are always successful, there are a total of $r(t - u)$ erasures across all users and all time instances. Suppose that the adversary has full control over which users will experience erasures, and they choose to restrict these erasures to Γ of the t users. First, suppose $\Gamma < t - u + 1$. In this case, there are at least u users that have zero erasures, and we are done. Now, let $\Gamma \geq t - u + 1$. The average number of erasures per targeted user is $\frac{r(t-u)}{\Gamma}$.

We claim that at least $\Gamma - (t - u)$ users have at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ erasures. Suppose not, and that at least $\Gamma - [\Gamma - (t-u)] + 1 = t - u + 1$ users have strictly more than $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ erasures. If $\frac{r(t-u)}{t-u+1}$ is an integer, the total number of erasures across all users and time instances is strictly bounded below by $(t-u+1)\frac{r(t-u)}{t-u+1} = r(t - u)$. If it is not an integer, the total number of erasures would be bounded below by $(t - u + 1)\lceil \frac{r(t-u)}{t-u+1} \rceil > r(t - u)$. Both cases contradict that the total number of erasures is equal to (at most) $r(t - u)$.

Thus, at least $\Gamma - (t - u)$ users have at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ erasures. The $t - \Gamma$ non-targeted users have zero erasures. Thus, at least $t - \Gamma + (\Gamma - (t - u)) = u$ users have at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ erasures. $\square$

This upper bound on the number of erasures for some subset of $u = \lceil \gamma t \rceil$ users is tight if the adversary may choose which users to target, and if they are able to reliably erase their targeted users. Both are advantageous assumptions for the adversary; we note that they will not always be the case (see Section V for a channel case study without the latter property).

Example IV.3. *Consider the codebooks of Example IV.1 with $\gamma = \frac{u}{t} = \frac{2}{3}$. First consider the case were the adversary targets all users equally. A possible erasure pattern is given below:*

User 1	ε	ε	c_{11}	c_{12}	c_{11}	c_{12}
User 2	c_{22}	c_{21}	ε	ε	c_{21}	c_{22}
User 3	c_{31}	c_{32}	c_{32}	c_{32}	ε	ε

In this case, the decoder needs to be able to correct two erasures (per user) in order to correct two of the three users.

Next, we look at the case were the adversary focuses their efforts on $t - u + 1 = 2$ users. Per Lemma IV.2, this is the adversary's optimal strategy.

User 1	ε	ε	ε	c_{12}	c_{11}	c_{12}
User 2	c_{22}	c_{21}	c_{21}	ε	ε	ε
User 3	c_{31}	c_{32}	c_{32}	c_{32}	c_{31}	c_{32}

Here, the decoder needs to correct three erasures in order to correct two of the three users.

Remark IV.4. *According to Lemma IV.2, if we wish to design $C_{\varepsilon,j}$ with probability of γ partial correction error equal to zero, $d_{min}(C_{\varepsilon,j}) \geq \lfloor \frac{r(t-u)}{t-u+1} \rfloor + 1$ for each $j \in [t]$.*

Remark IV.4 addresses the requirement of perfect correction of $C_{\varepsilon,j}$. Allowing for some vanishing decoding error probability, we turn to the capacity of the induced erasure AVC.

Lemma IV.5. *Let $\gamma \in (0,1)$, $n \geq 1$, $t \geq 2$, and $W := W_{Y|X_1 \cdots X_t S}$ be a t-user AV-MAC. Suppose a γ partially correcting authentication code $(M_1, \ldots, M_t, n)$ exists for W such that $M_j := 2^{R_j n} > 1$ for all $j \in [t]$ and the probability of γ partial correction error is equal to zero. Then, $\mathscr{C}_{auth,\gamma}$ has nonempty interior.*

Proof. Choose a user $j \in [t]$, and define a deterministic erasure AVC as follows: let $\mathcal{X} = [M_j]$, $\mathcal{Y} = [M_j] \cup \{\varepsilon\}$, and $\mathcal{S} = \{s_0, s_1\}$. Then, $y = x$ if $s = s_0$, and $y = \varepsilon$ if $s = s_1$. Let $u := \lceil \gamma t \rceil$. Importantly, the adversary is power-constrained so that in a length-r transmission they may choose at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ coordinates to be equal to s_1; the remainder must be equal to s_0. There are no constraints on the legitimate user's channel input. This channel mimics the worst-case scenario for (at least) u users in the above-described concatenation scheme: each has at most $\lfloor \frac{r(t-u)}{t-u+1} \rfloor$ erasures, and in our induced channel we assume that any time the adversary attempts to erase a user they can do so successfully. We refer the reader to Theorem 3 of [5] to verify that this channel has positive capacity.

It remains to explain why this implies an achievable positive rate tuple for the original AV-MAC. For each user $j \in [t]$, let a code sequence $(2^{Q_j r}, r)$ achieve the capacity of the erasure AVC. Using the concatenation scheme described earlier in this section, with the existing zero-error γ partial correction code as inner code, we achieve rate $Q_j R_j > 0$ for user j. $\square$

The case study in [7] calculates the exact capacity of an induced erasure AVC, which is dependent on the AV-MAC studied there (and extended in Section V), as well as the specific choice of inner code for that channel. There, when the adversary acted they had a 0.5 probability of erasing, as opposed to the guaranteed erasure assumed in the proof of Lemma IV.5. In other words, we believe it is possible to be more specific about the values of the positive rate tuples achievable using our extension scheme. We plan to address this question, as well as the question of whether a less stringent inner code may be utilized, in a full version of this work.

V. ZERO PROBABILITY OF PARTIAL CORRECTION ERROR CODES CASE STUDY

In this section, we turn to a particular t-user channel satisfying the necessary conditions of Section III for authenticated partial correction. We will work to construct short block length codes with zero probability of γ partial correction error, with the knowledge that such codes can be extended using the scheme of Section IV. To define the channel, let

$\mathcal{X}_1 = \cdots = \mathcal{X}_t = \{0,1\}$, $\mathcal{S} = \{0,1,2,\ldots,\ell\}$ for some $\ell \geq 1$, and $\mathcal{Y} = \{0,1,\ldots,t+\ell\}$, where $Y = X_1 + X_2 + \cdots + X_t + S$. The no-adversary state is given by $s_0 = 0$. For ease of notation, we will denote this channel by $W_{t,\ell}^+$. Observe that $W_{t,\ell}^+$ is deterministic given a choice of state.

A. Necessary conditions are satisfied

We first verify that $W_{t,\ell}^+$ satisfies the necessary overwritability and symmetrizability conditions established in Section III.

Lemma V.1. *$W_{t,\ell}^+$ is not m-overwritable for any $m \in [t]$.*

Proof. Let $W := W_{t,\ell}^+$ and $m \in [t]$. Toward contradiction, assume the channel is m-user overwritable in the first m coordinates, and let P be the distribution guaranteed by the definition of overwritability. Let $x_1' = \cdots = x_m' = 1$, $x_1 = \cdots = x_t = 0$, and $y = 0$. Then,

$$\sum_{s=0}^{\ell} P(s | \underbrace{1,\ldots,1}_{m}) W(0 | \underbrace{0,\ldots,0}_{t}, s) =$$
$$W(0 | \underbrace{\overbrace{1,\ldots,1}^{m}, \overbrace{0,\ldots,0}^{t-m}}_{t}, 0) \quad (18)$$

On the left hand side, $W(0|0,\ldots,0,s) = 1$ if and only if $s = 0$; otherwise it is zero. Therefore, the left side is equal to $P(0|1,\ldots,1)$. On the right side, $W(0|1,\ldots,1,0,\ldots,0,0) = 0$. Thus, $P(0|1,\ldots,1) = 0$.

A similar argument with $x_1' = \cdots = x_m' = 1$, $x_1 = x_2 = \cdots = x_m = 1$, $x_{m+1} = \cdots = x_t = 0$, and $y = m$ yields $P(0|1,\ldots,1) = 1$. This is a contradiction because $P(0|1,\ldots,1)$ cannot be equal to both 0 and 1. Therefore, the channel is not m-user overwritable. $\square$

Recall that the other necessary condition for a t-user channel to be γ partially correcting is that the channel is not q-user symmetrizable for any $q \geq t - \lceil \gamma t \rceil$. The following establishes allowed values of γ given the adversary's power constraint ℓ.

Lemma V.2. *Let $\ell \leq t$. Then $W_{t,\ell}^+$ is q-user symmetrizable for any subset of q users exactly when $q \leq \ell$.*

Proof. Let $W := W_{t,\ell}^+$. First we show that the channel is q-user symmetrizable for $q \leq \ell$. Consider the following probability distribution: $P(s|x_1,...,x_q) = 1$ if $\sum_{i=1}^{q} x_i = s$, and 0 otherwise. Notice that because each $x_i \in \{0,1\}$, we have $0 \leq \sum_{i=1}^{q} x_i \leq q$. Because $q \leq \ell$, for a fixed choice of x_i's, $P(s|x_1,\ldots,x_q) = 1$ for exactly one choice of s. Using this distribution in Definition II.3, the left hand size yields $W(y|x_1,\ldots,x_t,\sum_{i=1}^{q} x_i')$, and the right hand size becomes $W(y|x_1',\ldots,x_q',x_{q+1},\ldots,x_t,\sum_{i=1}^{q} x_i)$. The sum of the inputs will be the same on both sides, so either both sides are equal to 1 if the sum of the inputs is equal to y or both sides are equal to 0 if the sum of the inputs is not equal to y. Therefore, the channel is q-user symmetrizable for the first q users. Notice that permuting the coordinates will not change the argument, so we have shown that the channel is q-user symmetrizable for any subset of q users.

Now we will show the channel is *not* q-user symmetrizable when $\ell + 1 \le q \le t$. By way of contradiction, assume the channel is q-user symmetrizable for such a q. Let P be the distribution guaranteed by Definition II.3, and let $z \in S$ (note that $z \le \ell < t$). We claim that $P(z|0, ..., 0) = 0$. Assume $x_1' = \ldots = x_q' = 0$, $x_1 = \ldots = x_{t-z} = 1$, $x_{t-z+1} = \ldots = x_t = 0$, and $y = t$. Then, the left hand side of the definition is the sum over $s \in S$ of

$$P(s|\underbrace{0,\ldots,0}_{q})W(t|\overbrace{\underbrace{1,\ldots,1}_{t},0,\ldots,0}^{t-z}, s) \qquad (19)$$

and the right hand side is equal to the sum over $s \in S$ of

$$P(s|\overbrace{\underbrace{1,\ldots,1}_{q},0,\ldots,0}^{\min\{t-z,q\}})W(t|\overbrace{0,\ldots,0}^{q},\overbrace{\underbrace{1,\ldots,1}_{t},0,\ldots,0}^{((t-z)-q)^+}, s) \qquad (20)$$

where we use λ^+ to denote $\max\{\lambda, 0\}$. In Equation (19), $W(t|1,\ldots,1,0,\ldots,0,s) = 1$ if and only if $s = z$. Therefore, (19) is equal to $P(z|0,\ldots,0)$. In Equation (20), $W(t|0,\ldots,0,1,\ldots,1,0,\ldots,0,s) = 1$ if and only if $t = (t - z - q)^+ + s$. Since $s \le \ell < q \le t$, it follows that $s - q < 0$, and also $s < t$. Thus, $(t - z - q)^+ + s < t$, and (20) equals 0. Therefore, $P(z|0,\ldots,0) = 0$ for all $0 \le z \le \ell$, a contradiction. Therefore, no such P exists and the channel is not q-user symmetrizable for $\ell + 1 \le q \le t$. $\qquad \square$

Lemmas V.1 and V.2 together establish the following:

Theorem V.3. *The channel $W_{t,\ell}^+$ satisfies the necessary conditions for γ partial correction established by Theorem III.1, Lemma III.2, and Theorem III.3.*

B. Zero probability of γ partial correction characterization

To aid in our discussion of code construction, we next introduce notation that will help explain when a codebook is γ partially correcting with zero probability of error for $W_{t,\ell}^+$. Let $C_j := f_j(M_j)$ denote the block length n codebook of user j, so that each $\mathbf{x} \in C_j$ is equal to $f_j(i)$ for some $i \in M_j$. Then, define the following multisets:

$$A_0 := \left\{ \mathbf{u} = \sum_{j=1}^{t} \mathbf{x}_j \;\middle|\; \mathbf{x}_j \in C_j \right\} \qquad (21)$$

$$A_1 := \left\{ \mathbf{u} = \mathbf{s} + \sum_{j=1}^{t} \mathbf{x}_j \;\middle|\; \mathbf{x}_j \in C_j, \; \mathbf{s} \in S \setminus \{\mathbf{s}_0\} \right\} \qquad (22)$$

In other words, the set A_0 is the set of all possible channel outputs (with multiplicity) when the adversary does not act, and A_1 is the set of all outputs when the adversary does act.

Lemma V.4. *Over the channel $W_{t,\ell}^+$, a codebook t-tuple is γ partially correcting with zero probability of γ partial correction error if and only if all of the following hold:*

(1) $A_0 \cap A_1 = \emptyset$;
(2) The elements of A_0 are unique;

(3) For each $\mathbf{w} \in A_1$ that appears with multiplicity, there exists some subset $J = \{j_1, j_2, \ldots, j_{\lceil \gamma t \rceil}\} \subseteq [t]$ such that if $\mathbf{s} + \sum_{j=1}^{t} \mathbf{x}_j = \mathbf{w}$ and $\mathbf{s}' + \sum_{j=1}^{t} \mathbf{x}_j' = \mathbf{w}$, then $\mathbf{x}_i = \mathbf{x}_i'$ for all $i \in J$.

Proof. Condition (1) ensures that the decoder can reliably distinguish between the case where the adversary has acted and the case where they have transmitted a sequence of all zeros ($\mathbf{s}_0$). Taken together with (2), we have $e_\gamma(\mathbf{i}, \mathbf{s}_0) = 0$ for every message tuple $\mathbf{i}$. If either condition fails, $e_\gamma(\mathbf{i}, \mathbf{s}_0) > 0$.

With (1), condition (3) establishes that $e_\gamma(\mathbf{i}, \mathbf{s}) = 0$ when $\mathbf{s} \ne \mathbf{s}_0$: if there are repeated elements in A_1, we are guaranteed to be able to correct $\lceil \gamma t \rceil$ of the messages, even if the others must be discarded. If condition (3) fails, $e_\gamma(\mathbf{i}, \mathbf{s}) > 0$. $\qquad \square$

With this characterization in hand, we turn to short codebook design strategies. For the remainder of the paper, we will focus on the codebooks $C_j := f_j(M_j)$; thus, we will will discuss codebook tuples of the form $(C_1, \ldots, C_t)$.

C. Two users

Here we present necessary conditions for $\gamma = 0.5$ partially correcting codebook pairs over $W_{2,1}^+$ with zero probability of γ partial correction error, and bound the sizes of these codebooks for fixed block length.

Example V.5. *The codebook pair $C_1 = \{011, 100\}$, and $C_2 = \{010, 101\}$ is 0.5 partially correcting over $W_{2,1}^+$ with zero probability of γ partial correction error. This example was explored extensively in [7].*

The each codebook of Example V.5 has the property that codeword supports are not contained in one another. We find that this is true in general for partial correction over $W_{t,\ell}^+$.

Theorem V.6. *Let $(C_1, \ldots, C_t)$ be a codebook tuple with $C_j \in \{0,1\}^n$ for $j \in [t]$. If, for some $j \in [t]$, $\mathbf{x}, \mathbf{y} \in C_j$ with $\mathbf{x} \ne \mathbf{y}$ and $\mathrm{supp}(\mathbf{x}) \subseteq \mathrm{supp}(\mathbf{y})$, then the codebook tuple $(C_1, \ldots, C_t)$ is not γ partially correcting with zero probability of γ partial correction error over $W_{t,\ell}^+$ for any $\gamma \in (0,1)$.*

Proof. Let $\gamma \in (0, 1)$. Suppose that for some $j \in [t]$ there exist $\mathbf{x} \ne \mathbf{y} \in C_j$ such that $\mathrm{supp}(\mathbf{x}) \subseteq \mathrm{supp}(\mathbf{y})$. Let $\mathrm{supp}(\mathbf{y}) \setminus \mathrm{supp}(\mathbf{x})$ be the support of the adversarial contribution $\mathbf{s}$. Notice that $\mathbf{s} \in \{0,1\}^n \subseteq S^n$, and $\mathbf{s} + \mathbf{x} = \mathbf{y} + \mathbf{0}$. Thus $A_0 \cap A_1 \ne \emptyset$. By Lemma V.4, the result follows. $\qquad \square$

Let the partially ordered set (poset) $\mathcal{P}([n])$ be the power set of $[n]$ together with the partial order defined by set inclusion. Elements of the poset can alternatively be thought of as vectors in $\{0,1\}^n$; elements whose supports are contained in one another are then related under the partial order. Theorem V.6 states that each codebook of a γ partially correcting (with zero probability of γ partial correction error) codebook tuples are antichains (sets of unrelated elements) in $\mathcal{P}([n])$. The following corollary is a direct consequence of Theorem V.6.

Corollary V.7. *Suppose the codebook tuple $(C_1, \ldots, C_t)$ is γ partially correcting with zero probability of γ partial*

correction error over $W_{t,\ell}^+$ for some $\gamma \in (0,1)$. If $|C_j| > 1$, then $\mathbf{0}, \mathbf{1} \notin C_j$.

While each individual codebook must be an antichain, the disjoint union of codebooks need not be. Indeed, Example V.5 has two (disjoint) related pairs across codebooks. The following places a limit on such support containment.

Theorem V.8. *Let (C_1, C_2) be a 0.5 partially correcting codebook pair with zero probability of γ partial correction error over $W_{2,1}^+$. Provided $|C_1|, |C_2| > 1$, $C_1 \cap C_2 = \emptyset$ and $C_1 \sqcup C_2$ has at most two pairs of related codewords having the property that the intersection of these pairs is empty.*

Proof. Let (C_1, C_2) be a 0.5 partially correcting codebook pair with zero probability of γ partial correction error over $W_{2,1}^+$ and $|C_1|, |C_2| > 1$. To show that the codebooks are disjoint, suppose $\mathbf{x} \in C_1 \cap C_2$. Let $\mathbf{a} \neq \mathbf{x} \in C_1$ and $\mathbf{b} \neq \mathbf{x} \in C_2$. Note that $\mathbf{a}, \mathbf{b}, \mathbf{x} \in \mathcal{S}^n$. Observe that if either $[\mathbf{x}_1 = \mathbf{x}, \mathbf{x}_2 = \mathbf{b}, \mathbf{s} = \mathbf{a}]$, or $[\mathbf{x}_1 = \mathbf{a}, \mathbf{x}_2 = \mathbf{x}, \mathbf{s} = \mathbf{b}]$, the channel output is $\mathbf{x} + \mathbf{b} + \mathbf{a}$. This violates condition (3) of Lemma V.4. We have thus established that $C_1 \cap C_2 = \emptyset$.

Next, we will show that if there are two related pairs in the union, they have a particular structure. Let $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2 \in C_1 \sqcup C_2$ be distinct such that $\mathbf{x}_1 \leq \mathbf{x}_2$ and $\mathbf{y}_1 \leq \mathbf{y}_2$. Making use of Theorem V.6, and without loss of generality, we have two cases: either $\mathbf{x}_1, \mathbf{y}_1 \in C_1$, or $\mathbf{x}_1, \mathbf{y}_2 \in C_1$.

Suppose $\mathbf{x}_1, \mathbf{y}_1 \in C_1$ and $\mathbf{x}_2, \mathbf{y}_2 \in C_2$. Let $\mathbf{a}, \mathbf{b} \in \mathcal{S}^n$ be such that $\mathbf{x}_1 + \mathbf{a} = \mathbf{x}_2$ and $\mathbf{y}_1 + \mathbf{b} = \mathbf{y}_2$. Then,

$$\mathbf{x}_1 + \mathbf{y}_2 + \mathbf{a} = \mathbf{x}_2 + \mathbf{y}_2 = \mathbf{y}_1 + \mathbf{x}_2 + \mathbf{b}, \quad (23)$$

contradicting condition (3) of Lemma V.4. Thus, it must be the case that the two smaller elements, $\mathbf{x}_1$ and $\mathbf{y}_1$, must be in distinct codebooks.

Now suppose that $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2, \mathbf{z}_1, \mathbf{z}_2 \in C_1 \sqcup C_2$ are distinct elements with $\mathbf{x}_1 \leq \mathbf{x}_2$, $\mathbf{y}_1 \leq \mathbf{y}_2$, $\mathbf{z}_1 \leq \mathbf{z}_2$. Based on our above structural argument, $\mathbf{x}_1$, $\mathbf{y}_1$, and $\mathbf{z}_1$ must pairwise belong to different codebooks, an impossibility. $\square$

Theorem V.8 implies an upper bound on the size of the disjoint union:

Theorem V.9. *Let (C_1, C_2) be a 0.5 partially correcting codebook pair with zero probability of γ partial correction error over $W_{2,1}^+$, with $|C_1|, |C_2| > 1$. Then $|C_1 \sqcup C_2| \leq \binom{n}{\lceil n/2 \rceil} + 2$.*

Proof. From Sperner's theorem, the size of a largest antichain in $\mathcal{P}([n])$ is $\binom{n}{\lceil n/2 \rceil}$. From Theorem V.8, $C := C_1 \sqcup C_2$ will have the form of an antichain with at most two additional elements. The result follows. $\square$

D. Three or more users

With the goal of constructing short codebook tuples with zero probability of γ partial correction error over $W_{t,\ell}^+$ for $t \geq 3$, in this section we develop equivalent conditions for (1) and (3) of Lemma V.4 which are easier to check computationally. In particular, we will reinterpret these conditions in terms of differences of sums of legitimate codewords. This allows us to avoid actually constructing A_1, and to instead check conditions on the elements of A_0 (i.e. sums of codewords).

In each of the results of this section, we will consider two such sums: $\mathbf{u} = \sum_{j=1}^t \mathbf{x}_j$ and $\mathbf{v} = \sum_{j=1}^t \mathbf{y}_j$, where (not necessarily distinct) $\mathbf{x}_j, \mathbf{y}_j \in C_j$ are vectors of length n for each $j \in [t]$.

Lemma V.10. *Let $(C_1, \ldots, C_t)$ be a codebook tuple for the channel $W_{t,\ell}^+$, where $\ell \geq 1$. There exist distinct $\mathbf{u}, \mathbf{v} \in A_0$ such that $\mathbf{u} - \mathbf{v}$ is in $\{0, \ldots, \ell\}^n = \mathcal{S}^n$ if and only if $A_0 \cap A_1 \neq \emptyset$.*

Proof. Suppose the vector difference $\mathbf{u} - \mathbf{v} \in \{0, \ldots, \ell\}^n$ for some choice of $\mathbf{u}, \mathbf{v} \in A_0$. In this case, $\mathbf{u} - \mathbf{v}$ is an element in $\mathcal{S}^n$ not equal to $\mathbf{s}_0$; call this difference $\mathbf{s}$. Then, $\mathbf{u} = \mathbf{v} + \mathbf{s}$. We then see that $\mathbf{u} \in A_1$ and $\mathbf{u} \in A_0$. This means that $A_0 \cap A_1 \neq \emptyset$. On the other hand, let $\mathbf{u}$ be an element of nonempty $A_0 \cap A_1$. Since $\mathbf{u} \in A_1$, it must be the case that $\mathbf{u} = \mathbf{v} + \mathbf{s}$ for some $\mathbf{v} \in A_0$, $\mathbf{s} \neq \mathbf{s}_0$. Then, $\mathbf{u} - \mathbf{v} \in \mathcal{S}^n$, and we are done. $\square$

The following two examples illustrate Lemma V.10.

Example V.11. *Consider the set of three codebooks with block length $n = 6$ given below:*

$$C_1 = \{100110, 110110\} \quad (24)$$
$$C_2 = \{111010, 100101\} \quad (25)$$
$$C_3 = \{011111, 001010\} \quad (26)$$

We claim that $A_0 \cap A_1 \neq \emptyset$ over $W_{3,\ell}^+$ for this codebook. Let $\mathbf{u}, \mathbf{v} \in A_0$ be given by

$$\mathbf{u} = 100110 + 111010 + 011111 = 222231 \quad (27)$$
$$\mathbf{v} = 110110 + 100101 + 001010 = 211221 \quad (28)$$

Then, $\mathbf{u} - \mathbf{v} = 222231 - 211221 = 011010$. Here, we can see that $\mathbf{u} - \mathbf{v}$ is an element in $\mathcal{S}^n$ for any $\ell \geq 1$. Observe that $\mathbf{u} = \mathbf{v} + \mathbf{s}$ when $\mathbf{s} = 011010$, so that $A_0 \cap A_1 \neq \emptyset$ and condition (1) of Lemma V.4 fails.

Example V.12. *Consider the set of three codebooks with block length $n = 6$ given below:*

$$C_1 = \{011010, 100101\} \quad (29)$$
$$C_2 = \{010110, 101001\} \quad (30)$$
$$C_3 = \{001101, 110010\} \quad (31)$$

We claim that $A_0 \cap A_1 = \emptyset$ over $W_{3,\ell}^+$ for this codebook. Consider the following choice of $\mathbf{u}$ and $\mathbf{v}$ as an example:

$$\mathbf{u} = 011010 + 010110 + 001101 = 022221 \quad (32)$$
$$\mathbf{v} = 100101 + 101001 + 110010 = 311112 \quad (33)$$

Then,

$$\mathbf{u} - \mathbf{v} = 022221 - 311112 = (-3)1111(-1) \quad (34)$$

Here we can see that $\mathbf{u} - \mathbf{v}$ is not an element in $\mathcal{S}^n$. All values of $\mathbf{u} - \mathbf{v}$ can be looped through for this channel to show that $A_0 \cap A_1 = \emptyset$.

Next, we rephrase condition (3) of Lemma V.4 in terms of elements of A_0.

Lemma V.13. *Let $(C_1, \ldots, C_t)$ be a codebook tuple for the channel $W_{t,\ell}^+$, where $\ell \geq 1$, and let $\gamma \in (0,1)$. Let $\mathbf{u}, \mathbf{v} \in A_0$ such that $\mathbf{u} = \sum_{j=1}^t \mathbf{x}_j$ and $\mathbf{v} = \sum_{j=1}^t \mathbf{y}_j$ and $\mathbf{x}_j \neq \mathbf{y}_j$ for at least $t - \lceil \gamma t \rceil + 1$ values of $j \in [t]$. If the maximum entry of $|\mathbf{u} - \mathbf{v}|$ is at most ℓ, condition (3) of Lemma V.4 fails.*

Proof. Let $(C_1, \ldots, C_t)$ be a codebook tuple for the channel $W_{t,\ell}^+$, where $\ell \geq 1$, and let $\gamma \in (0,1)$. Let $\mathbf{u}, \mathbf{v} \in A_0$ such that $\mathbf{u} = \sum_{j=1}^t \mathbf{x}_j$ and $\mathbf{v} = \sum_{j=1}^t \mathbf{y}_j$ and $\mathbf{x}_j \neq \mathbf{y}_j$ for at least $t - \lceil \gamma t \rceil + 1$ values of $j \in [t]$. If the maximum entry of $|\mathbf{u} - \mathbf{v}|$ is $\leq \ell$, then $|\mathbf{u} - \mathbf{v}| \in \mathcal{S}^n$. Thus, $|\mathbf{u} - \mathbf{v}| = \mathbf{s}$ and $u_i - v_i = \pm s_i$ for each $i \in [n]$. Letting $\mathbf{s}_1$ equal $\mathbf{s}$ on coordinates where $u_i - v_i$ is negative, and zero elsewhere, and $\mathbf{s}_2 = \mathbf{s}$ when $u_i - v_i$ is positive, and zero elsewhere, we have $\mathbf{u} + \mathbf{s}_1 = \mathbf{v} + \mathbf{s}_2$. Condition (3) fails because the sums cannot match on any subset of $\lceil \gamma t \rceil$ codewords. $\square$

The following example illustrates Lemma V.13.

Example V.14. *Consider the set of three codebooks with block length $n = 6$ given below:*

$$C_1 = \{011010, 100101\} \tag{35}$$
$$C_2 = \{010110, 101001\} \tag{36}$$
$$C_3 = \{010101, 101010\} \tag{37}$$

We claim that condition (3) of Lemma V.4 fails over $W_{3,\ell}^+$ when $\gamma = \frac{1}{3}$ or $\gamma = \frac{2}{3}$. Let $\mathbf{u}, \mathbf{v} \in A_0$ be

$$\mathbf{u} = 100101 + 010110 + 101010 = 211221 \tag{38}$$
$$\mathbf{v} = 011010 + 101001 + 010101 = 122112 \tag{39}$$

It can be seen that $\mathbf{u}$ and $\mathbf{v}$ differ on all three users.

$$|\mathbf{u} - \mathbf{v}| = |211221 - 122112| = 111111 \tag{40}$$

and $\mathbf{u} - \mathbf{v} = 1(-1)(-1)11(-1)$ such that $\mathbf{u} + 011001 = \mathbf{v} + 100110$. Thus, condition (3) fails due to the fact that there is a repeated element in A_1 for which no user codewords match.

We observe that condition (2) of Lemma V.4 is straightforward to check on A_0 alone. Combining all checks on A_0 described in this section, we can algorithmically loop through the possible combinations of differences of elements of A_0 to test whether a codebook triple is a candidate for partial correction with zero probability of γ partial correction error. Notably, the check of Lemma V.13 is necessary (for some such $\mathbf{u}, \mathbf{v}$) for failure of condition (3) when there are three users and $\gamma = \frac{2}{3}$. In fact, the codebook given in Example V.12 is a good codebook triple for $W_{3,1}^+$ with $\gamma = \frac{2}{3}$. The extension scheme of Section IV can thus be used to achieve positive rate triples with arbitrary block length.

VI. Conclusion

In this paper, we gave necessary (non-)symmetrizability and (non-)overwritability conditions for nonempty interior of the γ partially correcting authentication capacity region over a t-user AV-MAC. We presented a scheme to extend the block length of a strong short block length code, showing that the resulting extension can maintain the positive rates of the short code. Finally, we examined the particular AV-MAC denoted $W_{t,\ell}^+$, deriving structural results and bounds for zero γ partial correction error codes over this channel. Ongoing and future directions include sufficiency of the aforementioned necessary channel conditions for partial correction, refinement of our block length extension scheme, and alternative paths toward inner bounds on the γ partially correcting authentication capacity region.

References

[1] J.-H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. on Inf. Theory*, vol. 27, no. 2, pp. 212–226, 1981.
[2] J. A. Gubner, "On the deterministic-code capacity of the multiple-access arbitrarily varying channel," *IEEE Trans. on Inf. Theory*, vol. 36, no. 2, pp. 262–275, 1990.
[3] R. Ahlswede and N. Cai, "Arbitrarily varying multiple-access channels. I. Ericson's symmetrizability is adequate, Gubner's conjecture is true," *IEEE Trans. on Inf. Theory*, vol. 45, no. 2, pp. 742–749, 1999.
[4] U. Pereg and Y. Steinberg, "The capacity region of the arbitrarily varying mac: with and without constraints," in *IEEE Int'l Symp. on Inf. Theory*, 2019, pp. 445–449.
[5] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Trans. on Inf. Theory*, vol. 34, no. 2, pp. 181–193, 1988.
[6] O. Kosut and J. Kliewer, "Authentication capacity of adversarial channels," in *IEEE Inf. Theory Workshop (ITW)*, 2018, pp. 1–5.
[7] A. Beemer, E. Graves, J. Kliewer, O. Kosut, and P. Yu, "Authentication and partial message correction over adversarial multiple-access channels," in *IEEE Conf. on Comm.s and Network Sec.*, 2020, pp. 1–6.
[8] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Multiple access channels with adversarial users," in *IEEE Int'l Symp. on Inf. Theory*, 2019, pp. 435–439.
[9] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Byzantine multiple access channels–part II: Communication with adversary identification," *arXiv preprint 2309.11174*, 2023.
[10] S. Nitinawarat, "On the deterministic code capacity region of an arbitrarily varying multiple-access channel under list decoding," *IEEE Trans. on Inf. Theory*, vol. 59, no. 5, pp. 2683–2693, 2013.
[11] N. Cai, "List decoding for arbitrarily varying multiple access channel revisited: List configuration and symmetrizability," *IEEE Trans. on Inf. Theory*, vol. 62, no. 11, pp. 6095–6110, 2016.