On Modulo-Sum Computation over an Erasure Multiple Access Channel

Ashish Khisti
Electrical and Computer Engineering Dept.
University of Toronto, Canada
Email: akhisti@comm.utoronto.ca

Brett Hern and Krishna Narayanan
Electrical and Computer Engineering Dept.
Texas A&M, College Station, TX, USA
Email: {krn@tamu.edu, hernbrem@neo.tamu.edu}

Abstract—We study computation of a modulo-sum of two binary source sequences over a two-user erasure multiple access channel. Each sender observes an independent and equiprobable binary sequence and the receiver is interested in computing the modulo-sum of the two sequences. The channel is modeled as a binary-input, erasure multiple access channel, which can be in one of three states — either the channel output is a modulo-sum of the two input symbols, or the channel output equals the input symbol on the first link and an erasure on the second link, or it equals the input symbol on the second link and an erasure on the first link. The associated state sequence is independent and identically distributed. We establish upper and lower bounds on the modulo-sum capacity. Our coding scheme uses either the compute-and-forward or the decode-and-forward techniques. The upper bound is obtained by a genie aided argument that reduces the setup to a compound multiple-access channel. It is in general is tighter than a simple upper bound obtained by revealing one of the messages to the decoders. We also briefly consider the case when a strictly causal state feedback is available to the encoders and establish that such feedback can increase the modulo-sum capacity.

I. INTRODUCTION

Many problems in network information theory require that the intermediate relay nodes only compute a function of the underlying source messages. One such example is the two-way relay channel where two users need to communicate to each other using a central relay node. It is natural that the relay node only compute a modulo-sum of the messages of the two users. In a classic paper, Korner and Marton [4] consider a multi-terminal source coding problem where the destination terminal is required to compute a modulo-sum of two binary sources. Each source is revealed to one encoder. The authors establish the optimality of a scheme using identical linear codebooks to separately compress the two source sequences. There has been a significant interest in source and channel coding techniques for function computation in recent times; see e.g. [1]–[3], [5]–[13].


The authors observe that for a wide range of signal-to-noise ratio (SNR), one can achieve higher rates using lattice codes instead of an i.i.d. random code ensemble. The additive nature, the Gaussian MAC channel is well suited for computing the modulo sum of two messages using lattice codes. A simple upper bound obtained by revealing one of the messages to the destination, is sufficiently close to the known lower bounds for a wide range of SNR. Several interesting extensions along these lines are also discussed in [6], [11].

In the present paper we introduce a MAC channel model that does not appear naturally matched for computing the modulo-sum function. Our model is an erasure multiple access channel with binary inputs. With a certain probability, the destination observes a modulo-sum of the two transmitted bits whereas with a certain probability the destination observes only one of the two bits and an erasure symbol associated with the other transmitted bit. As our main result, we establish that the cut-set upper bound is not tight and develop a new upper bound. We also briefly consider the case when there is strictly causal feedback of the state sequence available from the destination (using e.g., ARQ) and show that the capacity can be increased compared to the case without such a feedback.

II. PROBLEM STATEMENT AND MAIN RESULTS

We study a multiple access channel with two transmitters and one receiver. The channel input symbols are denoted by \( x \) and \( y \) respectively and are binary valued. The channel output is denoted by \( z \) and is also binary valued. The channel transition probability is controlled by a state variable \( s \in \{0, 1, 2\} \). In particular we have:

\[
    z = \begin{cases} 
    x \oplus y, & s = 0, \\
    x, & s = 1, \\
    y, & s = 2. 
    \end{cases} \tag{1}
\]

We assume that the receiver is revealed the pair \((z, s)\). We assume that \( \Pr(s = 1) = \Pr(s = 2) = \varepsilon \) and \( \Pr(s = 0) = 1 - 2\varepsilon \) where \( \varepsilon \) satisfies \( 0 \leq \varepsilon \leq 1/2 \). The channel is memoryless i.e., \( \Pr(s^n = s^n) = \prod_{i=1}^n \Pr(s_i = s_i) \) is satisfied.

A code of length \( n \) is defined as follows. Sender \( i \) observes a message \( w_i \) uniformly and independently distributed over the set \([1, \ldots, 2^{nR_i}]\). For sake of convenience we will represent
message \( w_i \) as a sequence \( b_{i}^{nR} \) consisting of \( nR \) independent and equiprobable bits. We define \( u = w_1 \oplus w_2 \) as the exclusive-or of \( b_{1}^{nR} \oplus b_{2}^{nR} \).

The messages are mapped into codewords \( x^n = f_n(w_i) \) and \( y^n = g_n(w_2) \) respectively and the decoder is required to produce \( \hat{u} = h_n(z^n, s^n) \). An error is declared if \( \{u \neq \hat{u}\} \).

A rate \( R \) is achievable if there is a sequence of encoders and decoders such that the error probability goes to zero as \( n \) approaches infinity. The largest achievable rate is defined as the modulo-sum capacity.

Remark 1: In this paper we focus on the simplified model in (1) where the channel can only take one of three states. The results can be extended to the case when there are two additional states — either the decoder observes both \((x, y)\) or it observes an erasure. Such extensions will be reported elsewhere.

We summarize the main results in the remainder of this section.

A. Lower Bound

We propose the following lower bound on the modulo-sum capacity.

**Proposition 1**: The modulo-sum capacity of the multiple-access erasure channel (1) is lower bounded by the following expression:

\[
C \geq R^- = \max \left\{ 1 - 2\varepsilon, \frac{1}{2} \right\}.
\]

The lower bound of \( R = 1 - 2\varepsilon \) is attained using a compute-and-forward technique [6]. The lower bound \( R = 1/2 \) is attained using a standard multiple-access channel code to transmit both \( w_1 \) and \( w_2 \) to the destination. This technique is referred to as decode-and-forward in this paper. The coding technique discussed in [3], which uses identical codebooks at the two transmitters also suffices to achieve this rate.

B. Upper Bound

We provide the following upper bound on the modulo-sum capacity.

**Theorem 1**: The modulo-sum capacity of the multiple-access erasure channel (1) is upper bounded by the following expression:

\[
C \leq R^+ = \frac{(1 - 3\varepsilon)^+ + (2 - \varepsilon)}{3}
\]

where \((\cdot)^+\) equals zero if the argument inside is negative.

The proposed upper bound is tighter than a genie-aided bound where one of the messages, say \( \hat{w}_1 \), is revealed to the decoder. We provide some intuition behind the upper bound below.

1) Revealing Side Information to the Transmitters: Our key idea is to reveal part of the state sequence to the encoders. In particular define the sets \( A = \{i : s_i = 1\} \) and \( C = \{i : s_i = 0\} \). We illustrate the technique when \(|A| = |B| = |C| = \frac{n}{3}\), which roughly corresponds to the case when \( \varepsilon = 1/3 \). We will use the notation \( z^C_i \) to denote the projection of \( z^n \) onto the indices \( i \in C \) etc.

In our upper bound, we first reveal the knowledge of \( B \) to the two encoders non-causally. However the encoders are not aware of the sets \( A \) and \( C \). Note from (1) that \( z^A_B = y^B_B \), \( z^A_C = x^C_A \) and \( z^C_C = x^C_C \oplus y^C_C \).

2) Independence of Input Signals from \( w_1 \oplus w_2 \): Observe that \( y^B_B \) is a sub-sequence transmitted by user 2 and hence independent of \( u = w_1 \oplus w_2 \). Using this property we have:

\[
nR = H(u)
\]

\[
\leq H(u | y^B_B) + I(x^B_A, z^C_B; u | y^B_B) + n \cdot o_n(1),
\]

where we use Fano’s inequality in \( \frac{1}{n} H(u | x^B_A, y^B_B, y^C_B) \leq o_n(1) \) and \( o_n(1) \) denotes a vanishing function in \( n \).

3) Compound MAC Channel: Observe that the same coding scheme must also work when the positions of sets \( A \) and \( C \) are interchanged. This results in

\[
nR \leq nR = H(u | y^B_B) + n \cdot o_n(1).
\]

Combining (7) and (8) and ignoring the \( o_n(1) \) term, we obtain the following:

\[
nR \leq nR = H(x^B_A, z^C_B | y^B_B, u) + n \cdot o_n(1).
\]

4) Penalty from Repetition Coding: Suppose that the sequence \( x^n \) is completely revealed to the destination. The receiver only needs to compute \( w_2 \) and hence we have:

\[
nR \leq H(y^n) = H(y^A_A, y^C_C | y^B_B) + H(y^B_B)
\]

Eliminating the joint entropy term between (14) and (15) we get

\[
\frac{3}{2} nR \leq \frac{1}{2}H(y^B_B) + n(1 - \varepsilon)
\]

By using the simple upper bound \( H(y^B_B) \leq |B| = n\varepsilon \) we get \( R \leq \frac{2}{3\varepsilon} \) which agrees with (3) for \( \varepsilon = 1/3 \).
C. Causal State Feedback

Consider the case when the encoders are revealed the state sequences in a strictly manner. The encoding functions at time $i$ can depend on the state sequence up to time $i-1$ i.e. $x_i = f_i(w_1, s_i^{-1})$ and $y_i = g_i(w_2, s_i^{-1})$.

Proposition 2: The modulo-sum capacity the multiple access channel with strictly causal state feedback is lower and upper bounded by $R_{FB}^r \leq C \leq R_{FB}^+$, where

$$\begin{align*}
R_{FB}^- &= \frac{1}{1+2\varepsilon} \quad (17) \\
R_{FB}^+ &= 1 - \varepsilon \quad (18)
\end{align*}$$

The lower bound is achieved by a two-phase protocol where the users transmit uncoded bits in the first phase and use a multiple-access code in the second phase. The upper bound is the genie-aided bound where one of the messages is revealed to the destination. The problem reduces to communicating the other message, say $w_2$ to the destination. Feedback in such a case is well known to not increase the point-to-point capacity.

III. LOWER BOUND: PROOF OF PROP. 1

We separately establish the achievability of $R = 1 - 2\varepsilon$ and $R = 1/2$.

A. Compute and Forward Scheme

We use identical linear codebooks at the two transmitters in the compute and forward scheme to achieve $R = 1 - 2\varepsilon$. Recall that the messages $w_1$ and $w_2$ are assumed to be binary valued sequences of length $nR$ bits i.e., we take

$$b_i^T = [b_{i1}, \ldots, b_{iK}]$$

where $K = nR$ denote the number of information bits in the message. Let $G$ be a matrix of dimensions $K \times n$, and let each entry in $G$ be sampled independently from an equiprobable Bernoulli distribution. It is useful to express

$$G = [g_1, \ldots, g_n]$$

where each $g_i \in \{0, 1\}^K$ is a length $K$ binary valued column vector. The transmitted sequence $x^T = [x_1, \ldots, x_K]$ at receiver 1 is expressed as:

$$x^T = b_1^T \cdot G$$

$$= [b_1^T g_1, \ldots, b_1^T g_n]$$

The transmitted sequence $y^T$ at user 2 is defined in a similar manner.

The receiver is interested in computing

$$u^T = b_1^T \oplus b_2^T = [b_{11} \oplus b_{21}, \ldots, b_{1K} \oplus b_{2K}].$$

Given our specific encoder, the received symbol can be expressed as:

$$z_i = \begin{cases} 
(b_1^T \oplus b_2^T)g_{i1}, & s_i = 0, \\
b_1^T g_i, & s_i = 1, \\
b_2^T g_i, & s_i = 2.
\end{cases} \quad (24)$$

Our proposed decoder only uses the output of the channel when $s_i = 0$ and declares erasures if $s_i \neq 0$. Let $\hat{G}_0 = G_{|s_i=0}$ be collection of column vectors in $G$ when $s_i = 0$. We use the following lemma regarding $\hat{G}_0$:

Lemma 1: For every $\delta > 0$, there exists a function $\alpha_n(\delta)$ that goes to zero as $n \to \infty$, such that follows holds:

$$\Pr \left( \text{rank}(\hat{G}_0) \geq \min(K, n(1-2\varepsilon - \delta)) \right) \geq 1 - \alpha_n(\delta).$$

(25)

The proof of Lemma 1 is obtained by showing that, with high probability, each randomly selected column of $\hat{G}_0$ is in a general position. We omit the proof. Clearly the receiver can uniquely recover $(b_1^T \oplus b_2^T)$ from

$$z_o^T = (b_1^T \oplus b_2^T) \cdot \hat{G}_0$$

if $\hat{G}_0$ has full row-rank, which holds if $R \leq 1 - 2\varepsilon - \delta$. Since $\delta > 0$ is arbitrary this establishes our first lower bound.

B. Achievability of $R = 1/2$: Decode and Forward Approach

The rate $R = 1/2$ is achieved by transmitting both $w_1$ and $w_2$ to the destination instead of taking advantage of the fact that the destination only requires $w_1 \oplus w_2$. The multiple access capacity region is given by the convex hull of rate pairs $(R_1, R_2)$ that satisfy:

$$R_1 \leq I(x; z, s|y)$$

$$R_2 \leq I(y; z, s|x)$$

$$R_1 + R_2 \leq I(x, y; z, s)$$

Taking $x$ and $y$ to be independent equiprobable binary symbols we get that MAC Capacity region contains $R_1 \leq 1 - \varepsilon$, $R_2 \leq 1 - \varepsilon$ and $R_1 + R_2 \leq 1$. Since $\varepsilon < 1/2$ the rate pair $R_1 = R_2 = 1/2$ is achievable. Thus each user can transmit $w_i$ at a rate of $R = 1/2$ to the destination. The destination then computes $w_1 \oplus w_2$.

Remark 2: The rate $R = 1/2$ can be achieved using a decode and forward scheme even when the two transmitters use identical codebooks. As established in [3], in addition to (27)-(29), an additional constraint

$$R \leq I(x, y; z, s|x \oplus y) = 2\varepsilon$$

must be satisfied when identical codebooks are used. Thus the achievable rate now reduces to $R = \min(1/2, 2\varepsilon)$. Note that with identical codebooks, the rate $R = 1/2$ is achievable for $\varepsilon > 1/4$, the region in which decode and forward dominates compute and forward discussed before.

Achieving $R = 1/2$ with Compute and Forward: The rate $R = 1/2$ can also be achieved using identical linear codes if the receiver does not ignore the output when $s_i \neq 0$. Let $G_0 = G_{|s_i=0}$, $G_1 = G_{|s_i=1}$ and $G_2 = G_{|s_i=2}$ be the projections of $G$ onto the indices where $s_i = 0$, $s_i = 1$ and $s_i = 2$ respectively. Following (24), we let $z_i^T = (b_1^T + b_2^T)\hat{G}_0$, $z_1^A = b_1^T \hat{G}_1$ and $z_2^B = b_2^T \hat{G}_2$. Since the column vectors in $G_1$ and $G_2$ are independently sampled it can be shown that
for any $\delta > 0$, with a probability that exceeds $1 - o_n(1)$, we have that
\[
\dim \left( \text{col-space}(\hat{G}_1) \cap \text{col-space}(\hat{G}_2) \right) \geq n \cdot d_{12} - \delta n \cdot (2\varepsilon - R)^{+} \tag{30}
\] 
Thus one can find a matrices $M_i$ such that
\[
\hat{G}_1 M_1 = \hat{G}_2 M_2 = A \tag{31}
\]
where $A$ is a full-rank of dimension $n \times d_{12}$. The receiver first computes
\[
(z_A^T \oplus z_B^T) M = (b_1^T \oplus b_2^T) \cdot A \tag{32}
\]
and then needs to compute $b_1 \oplus b_2$ from $(b_1 \oplus b_2)^T \hat{G}_0 [A]$. Since the entries in $\hat{G}_0$ and $A$ are independent the rank of $[\hat{G}_0 \ A]$ is, with high probability at-least $n(d_{12} + 1 - 2\varepsilon - \delta)$. From (30) we can show that $R = \max(\frac{4}{9}, 1 - 2\varepsilon)$ is achievable.

### IV. Upper Bound: Proof of Theorem 1

We begin with some notation. For a given sequence $s^n$ $A(s^n) = \{i : s_i = 1\}$ and $B(s^n) = \{i : s_i = 2\}$. Let $C(s^n) = \{i : s_i = 0\}$. We let $x_{A(s^n)}$ to be the projection of the sequence $x^n$ on the indices where $s_i = 1$ and use a similar notation for other indices.

Since the receiver decodes $u = w_1 \oplus w_2$ from its output, from Fano’s inequality, we have that
\[
\frac{1}{n} H(u | s^n, z^n) \leq \delta_n \tag{33}
\]
for some sequence $\varepsilon_n$ that goes to zero as $n \to \infty$.

Now consider
\[
nR = H(u) = H(u | s^n) - I(u; x_{A(s^n)}), z_{C(s^n)} | s^n, y_{B(s^n)} \tag{34}
\]
\[
= H(u | s^n, y_{B(s^n)}) \tag{35}
\]
\[
= n\delta_n + I(u; x_{A(s^n)}, z_{C(s^n)} | s^n, y_{B(s^n)}) \tag{36}
\]
\[
= n\delta_n + H(x_{A(s^n)}, z_{C(s^n)} | s^n, y_{B(s^n)}) - H(x_{A(s^n)}, z_{C(s^n)} | s^n, y_{B(s^n)}), u) \tag{37}
\]
where (35) follows from the fact that the message $u$ is independent of the sequence $s^n$, equation (36) follows from the fact that $u = w_1 \oplus w_2$ is independent of $w_2$ and hence also independent of $y^n$, and equation (37) follows from the chain rule of mutual information and the application of Fano’s inequality.

We upper bound the first entropy term in (38) as follows.
\[
H(x_{A(s^n)}, z_{C(s^n)} | s^n, y_{B(s^n)}) \leq nH(x_{A(s^n)}, z_{C(s^n)} | s^n), \tag{39}
\]
\[
\leq \sum_{s^n \in S^n} \Pr(s^n) (|A(s^n)| + |C(s^n)|) \tag{40}
\]
\[
= n(1 - \varepsilon) + n\delta_n \tag{41}
\]
where (39) follows from the fact that conditioning reduces entropy whereas (40) follows from the fact that both $x^n$ and $z^n$ are binary sequences and (41) follows from the fact $s^n$ is sampled i.i.d. from a distribution with $\Pr(s = 0) = 1 - 2\varepsilon$ and $\Pr(s = 1) = \Pr(s = 2) = \varepsilon$.

Substituting (41) into (38) we have:
\[
nR \leq n(1 - \varepsilon) + n\delta_n - H(x_{A(s^n)}, z_{C(s^n)} | s^n, y_{B(s^n)}), u) \tag{42}
\]

In this paper we only provide the complete converse when $\Pr(s = 0) = \Pr(s = 1) = \Pr(s = 2) = \frac{1}{3}$. The proof for the general case also uses (42) as a starting point and will appear elsewhere.

For a sequence $s^n$ we first consider a permutation function $\pi(s^n)$ such that $A(s^n) = C(\pi(s^n)), B(s^n) = B(\pi(s^n))$, and $C(s^n) = A(\pi(s^n))$. Note that $\Pr(s^n = s^n) = \Pr(s^n = \pi(s^n)) = \frac{1}{3}$. We establish the following lower bound:
\[
H(x_{A(\pi(s^n))}, z_{C(\pi(s^n))} | y_{B(\pi(s^n))}, u, s^n) + \\
= H(x_{A(\pi(s^n))}, z_{C(\pi(s^n))} | y_{B(\pi(s^n))}, u, s^n) + \\
= H(y_{C(s^n)} | y_{B(s^n)}), u, s^n) \tag{43}
\]
\[
\geq H(x_{A(\pi(s^n))}, z_{C(\pi(s^n))} | y_{C(s^n)} | y_{B(\pi(s^n))}, u, s^n) \tag{44}
\]
\[
\geq H(y_{C(s^n)} | y_{A(\pi(s^n))} | y_{B(s^n)}), u, s^n) \tag{45}
\]
where (44) follows from the construction of the permutation function $\pi(\cdot)$, (45) follows from the fact that conditioning reduces entropy and the chain rule, (46) follows from the fact that $z^n = x^n \oplus y^n$ and for any random variable $A$ we have that $H(A) = H(f(A))$ if the function $f(\cdot)$ is one-to-one, while (48) follows from the fact that $u = w_1 \oplus w_2$ is independent of $w_2$ and hence of $y^n$.

Now applying (42) to the sequence $\pi(s^n)$ we get
\[
nR \leq n(1 - \varepsilon) + n\delta_n - \\
\leq n(1 - \varepsilon) + n\delta_n - \frac{1}{2} H(y_{C(s^n)} | y_{A(\pi(s^n))} | y_{B(s^n)}), u, s^n) \tag{49}
\]
Combining (42) and (49) we have:
\[
nR \leq n(1 - \varepsilon) + n\delta_n - \frac{1}{2} H(y_{C(s^n)} | y_{A(\pi(s^n))} | y_{B(s^n)}), u, s^n) \tag{50}
\]
To complete our analysis, we consider the upper bound by revealing $w_1$ to the decoder.
\[
nR = H(w_1 \oplus w_2) = H(w_2 | w_1) \tag{51}
\]
\[
= H(w_2 | w_1, s^n) \tag{52}
\]
\[
= H(w_2 | w_1, s^n, y^n) + I(y^n; w_2 | w_1, s^n) \tag{53}
\]
\[
\leq n\delta_n + H(y^n | s^n) \tag{54}
\]
hence Fano’s inequality implies, \(\epsilon\) is the lower bound achieved by either the decode and forward or the compute and forward schemes. The other solid curve is our new upper bound on the capacity without feedback (c.f. Theorem 1). The fourth curve is the lower bound with feedback in Prop. 2. Interestingly we see that it lies above the upper bound for certain values of \(\epsilon\), thus establishing that feedback helps in computation over the erasure multiple access channel.

### VII. Conclusion

We study computation of modulo-sum of two messages over a multiple access channel with erasures. Unlike the Gaussian model, our proposed this model does not have a suitable structure to directly compute the modulo-sum. Our main result is an upper bounding technique that reduces the setup to a compound multiple access channel. Using this bound we establish that a simple ARQ type feedback can increase the modulo-sum capacity. In the full paper we will report a complete derivation of the upper bound and other extensions such as the case of lossy recovery.

While computation over Gaussian networks has received a significant interest in recent years, we understand little about fundamental limits of computation over other channel models. We expect the ideas involved in this paper to be also applicable to other channel models.

### References


