Resolvability of the Multiple Access Channel with Two-Sided Cooperation

Noha Helal*, Matthieu Bloch† and Aria Nosratinia*
* The University of Texas at Dallas, 800 W Campbell Rd, Richardson, TX 75080, USA, {noha.helal, aria}@utdallas.edu
† Georgia Institute of Technology, North Ave NW, Atlanta, GA 30332, USA, matthieu.bloch@ece.gatech.edu

***Abstract*—We study the randomness required at the inputs of a multiple access channel in order to produce a desired, approximately i.i.d., output distribution, subject to cooperation in one of the following forms: (i) a common message, (ii) conferencing, (iii) feedback and (iv) generalized feedback. For the cases (i)-(iii), we characterize the channel resolvability via matching inner and outer bounds, and for generalized feedback we provide two inner bounds representing the role of decoding and randomness extraction, which can also be combined. One of the main contributions of this work is to show that resolvability rates of the multiple access channel are not improved with feedback, unlike the multiple access channel capacity which *is* improved by feedback.**

I. Introduction

The optimal amount of randomness at the input of a noisy channel required to approximate a distribution at the output is called channel resolvability; channel resolvability was first characterized in [1] building upon the work of [2] on the characterization of common information of two dependent random variables. While normalized Kullback-Leibler (KL) divergence was originally considered as a measure of approximation in [2], simplified proofs have later been developed for total variation [3] and non-normalized KL approximation [4].

Channel resolvability provides a powerful and general framework for solving various problems in information theory, including strong secrecy [5]–[8], covert communication [9], source coding [10], rate distortion theory [11] and coordination [3].

Channel resolvability in a multiple access channel (MAC) with non-cooperating encoders was studied in [12]–[15]. The role of user cooperation in enhancing channel resolvability was studied in [16] under perfect cooperation conditions, i.e., one user has access to the other user's transmitted signal noiselessly through cribbing as described by [17]. The role of cooperation in the presence of noisy communication in a multi-user setting, the relay channel, was studied in [18]. The work thus far on resolvability of cooperative multiple access channel has concentrated on various forms of *one-sided* cooperation. The key feature of the present work is that it studies distinct forms of cooperation that are *two-sided*, as well as their impact on the resolvability of multiple access channel.

The work of N. Helal and A. Nosratinia was supported in part by National Science Foundation (NSF) grant 1514050. The work of M. R. Bloch was supported by National Science Foundation (NSF) grant 1527074.

We study here the channel resolvability of the multiple access channel with various two-sided cooperating strategies, namely: (i) a common message, (ii) conferencing, (iii) feedback and (iv) generalized feedback. For the MAC with a common message, the MAC with conferencing and the MAC with feedback, we exactly characterize the channel resolvability via tight inner and outer bounds. For the MAC with feedback, one of the highlights of the present paper is a converse that shows feedback does not improve the resolvability of MAC. It is well known that feedback *does* improve the MAC capacity, thus MAC capacity and resolvability react differently to feedback.

We also show that tools previously developed in [16] and [18] can be generalized to prove resolvability results for the MAC with generalized feedback. We offer two achievable resolvability regions. The essence of the achievability proofs is carefully applying block-Markov encoding to handle the strict causality imposed by the channel feedback; randomness is appropriately recycled to break the dependence across blocks created by the encoding scheme. Furthermore, we harness the randomness that stems from the channel noise independent of the channel input [19] via a random binning argument to introduce fresh randomness at the encoders and assist in the approximation of the output distribution. Special cases of the derived resolvability region of the MAC with generalized feedback include the resolvability regions of the relay channel, the MAC with non-cooperating encoders and the MAC with strictly-causal cribbing.

The paper is organized as follows. Section II establishes the notation, Section III highlights the cooperation strategies and presents the achievable rate results for common messages, conferencing, and generalized feedback. Section IV provides the converse for MAC with feedback. Since this converse is tight against the results of [13], no new achievable rate is needed for MAC with feedback. Section V concludes the paper.

II. Notation

Random variables are represented by upper case letters and their realizations by the corresponding lower case letters. Superscripts denote the length of a sequence of symbols and subscripts denote the position of a symbol in a sequence. Calligraphic letters represent sets. P_X and P_{XY} denote probability distributions on $\mathcal{X}$ and $\mathcal{X} \times \mathcal{Y}$, respectively.

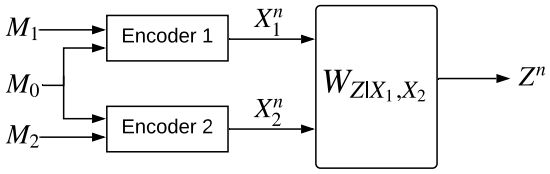

Fig. 1. The discrete memoryless MAC with common message.

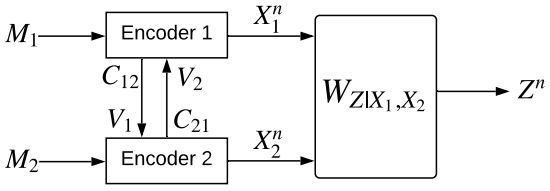

Fig. 2. The discrete memoryless MAC with conferencing.

For two distributions P and Q on the same finite alphabet $\mathcal{X}$, $\mathbb{D}(P\|Q)$ is the Kullback-Leibler (KL) divergence between P and Q defined by $\mathbb{D}(P\|Q) \triangleq \sum_x P(x)\log\frac{P(x)}{Q(x)}$. For a vector X^n with independent and identically distributed (i.i.d.) components $\{X_i\}_{i=1}^n$, distributed according to $P_X(x)$, we denote the product distribution of X^n by $P_X^{\otimes n}(x^n) \triangleq \prod_{i=1}^n P_X(x_i)$. log denotes the base 2 logarithm.

III. Cooperation Strategies

A. MAC with a Common Message

The discrete memoryless MAC with a common message (Fig. 1) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet $\mathcal{Z}$ with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2)W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 operating on uniformaly distributed inputs $M_0 \in [\![1, 2^{nR_0}]\!]$, $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_1 : \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{X}_1^n, \tag{1}$$

$$f_2 : \mathcal{M}_0 \times \mathcal{M}_2 \to \mathcal{X}_2^n. \tag{2}$$

Definition 1. *A rate tuple (R_0, R_1, R_2) is achievable for the discrete memoryless MAC with a common message $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate tuples (R_0, R_1, R_2).*

Theorem 1. *The resolvability region for the discrete-memoryless MAC with a common message is the set of rate tuples (R_0, R_1, R_2) such that*

$$R_0 \geqslant I(U;Z), \tag{3}$$

$$R_0 + R_1 \geqslant I(U, X_1; Z), \tag{4}$$

$$R_0 + R_2 \geqslant I(U, X_2; Z), \tag{5}$$

$$R_0 + R_1 + R_2 \geqslant I(X_1, X_2; Z), \tag{6}$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ with marginal Q_Z.

Proof. The proof is omitted for brevity. □

Remark 1. *The resolvability of the MAC with non-cooperating encoders [13] can be retrieved from Theorem 1 by setting $R_0 = 0$.*

Remark 2. *The resolvability of the MAC with degraded message sets [16], [20] can be retrieved from Theorem 1 by setting $R_1 = 0$, $R_0 = R_1$ and $U = X_1$.*

B. MAC with Conferencing

The discrete memoryless MAC with conferencing (Fig. 2) as introduced by Willems [21] consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet $\mathcal{Z}$ with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2)W_{Z|X_1,X_2}(z|x_1,x_2)$. A conference consists of K subsequent pairs of communications between the two encoders. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 operating on uniformly distributed inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$ and K conferencing functions g_{1k} and g_{2k} for $k \in [\![1, K]\!]$ defined as follows:

$$g_{1k} : \mathcal{M}_1 \times \mathcal{V}_2^{k-1} \to \mathcal{V}_{1k}, \text{ for } k \in [\![1, K]\!], \tag{7}$$

$$g_{2k} : \mathcal{M}_2 \times \mathcal{V}_1^{k-1} \to \mathcal{V}_{2k}, \text{ for } k \in [\![1, K]\!], \tag{8}$$

$$f_1 : \mathcal{M}_1 \times \mathcal{V}_2^K \to \mathcal{X}_1^n, \tag{9}$$

$$f_2 : \mathcal{M}_2 \times \mathcal{V}_1^K \to \mathcal{X}_2^n. \tag{10}$$

The amount of information exchanged during conferencing is bounded by the capacities C_{12} and C_{21} of the communication links between the encoders. C_{12} is the capacity of the link used by Encoder 1 to communicate to Encoder 2 and C_{21} is the capacity of the reverse link so that

$$\sum_{k=1}^K \log|\mathcal{V}_{1k}| \leqslant nC_{12}, \tag{11}$$

$$\sum_{k=1}^K \log|\mathcal{V}_{2k}| \leqslant nC_{21}. \tag{12}$$

Definition 2. *A rate pair (R_1, R_2) is achievable for the discrete memoryless MAC with conferencing $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with increasing block length such that $\lim_{n\to\infty} \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) = 0$. The MAC resolvability region is the closure of the set of achievable rate pairs (R_1, R_2).*

Theorem 2. *The resolvability region for the discrete-memoryless MAC with conferencing is the set of rate pairs (R_1, R_2) such that*

$$C_{12} + C_{21} \geqslant I(U;Z), \tag{13}$$

$$R_1 \geqslant I(U, X_1; Z) - C_{21}, \tag{14}$$

$$R_2 \geqslant I(U, X_2; Z) - C_{12}, \tag{15}$$

$$R_1 + R_2 \geqslant I(X_1, X_2; Z), \tag{16}$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ *with marginal* Q_Z.

Proof. We only provide a sketch of the proof. The idea behind the achievability proof is to convert this cooperation scheme into a setting that corresponds to a MAC with common message where the resolvability rates in (3)-(6) are achievable. Let us define the following rates

$$\tilde{R}_0 = C_{12} + C_{21}, \tag{17}$$

$$\tilde{R}_1 = R_1 - C_{12}, \tag{18}$$

$$\tilde{R}_2 = R_2 - C_{21}. \tag{19}$$

i.e., we defined the common message as the randomness exchanged via conferencing. Combining (3)-(6) and (17)-(19) yields the desired region. □

Remark 3. *The resolvability of the MAC with non-cooperating encoders [13] can be retrieved from Theorem 1 by setting* $C_{12} = C_{21} = 0$.

C. MAC with Feedback

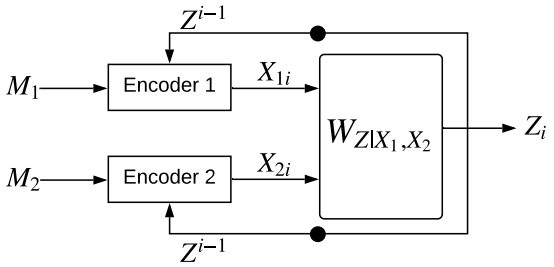

Fig. 3. The discrete memoryless MAC with feedback.

The discrete memoryless MAC with feedback (Fig. 3) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabet $\mathcal{Z}$ with a channel transition probability $W_{Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output is distributed according to $Q_Z(z) = \sum_{x_1,x_2} P_{X_1,X_2}(x_1,x_2) W_{Z|X_1,X_2}(z|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 operating on uniformly distributed inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_{1i} : \mathcal{M}_1 \times \mathcal{Z}^{i-1} \to \mathcal{X}_{1i}, \tag{20}$$

$$f_{2i} : \mathcal{M}_2 \times \mathcal{Z}^{i-1} \to \mathcal{X}_{2i}. \tag{21}$$

Definition 3. *A rate pair* (R_1, R_2) *is achievable for the discrete memoryless MAC with feedback* $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z|X_1,X_2}, \mathcal{Z})$ *if there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *codes with increasing block length such that* $\lim_{n\to\infty} \mathbb{D}(P_{Z^n} || Q_Z^{\otimes n}) = 0$. *The MAC resolvability region is the closure of the set of achievable rate pairs* (R_1, R_2).

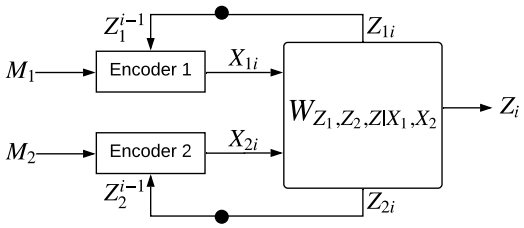

Fig. 4. The discrete memoryless MAC with generalized feedback.

Theorem 3. *The resolvability of the MAC with feedback is the set of rate pairs* (R_1, R_2) *such that:*

$$R_1 \geqslant I(X_1; Z|U),$$

$$R_2 \geqslant I(X_2; Z|U),$$

$$R_1 + R_2 \geqslant I(X_1, X_2; Z|U),$$

for some joint distribution $P_{U,X_1,X_2,Z} \triangleq P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ *with marginal* Q_Z.

Proof. See Section IV. □

We provide a converse proof and show that feedback does not improve the resolvability of the MAC.

D. MAC with Generalized Feedback

The discrete memoryless MAC with generalized feedback (Fig. 4) consists of finite input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and finite output alphabets $\mathcal{Z}_1$, $\mathcal{Z}_2$ and $\mathcal{Z}$ with a channel transition probability $W_{Z_1,Z_2,Z|X_1,X_2}$. For a joint distribution P_{X_1,X_2} on $\mathcal{X}_1 \times \mathcal{X}_2$, the output Z is distributed according to $Q_Z(z) = \sum_{x_1,x_2,z_1,z_2} P_{X_1,X_2}(x_1,x_2) W_{Z_1,Z_2,Z|X_1,X_2}(z_1,z_2,z|x_1,x_2)$. A $(2^{nR_1}, 2^{nR_2}, n)$ channel resolvability code consists of two encoders f_1 and f_2 operating on uniformly distributed inputs $M_1 \in [\![1, 2^{nR_1}]\!]$ and $M_2 \in [\![1, 2^{nR_2}]\!]$. The encoding functions are defined as follows:

$$f_{1i} : \mathcal{M}_1 \times \mathcal{Z}_1^{i-1} \to \mathcal{X}_{1i}, \tag{22}$$

$$f_{2i} : \mathcal{M}_2 \times \mathcal{Z}_2^{i-1} \to \mathcal{X}_{2i}. \tag{23}$$

Definition 4. *A rate pair* (R_1, R_2) *is achievable for the discrete memoryless MAC with generalized feedback* $(\mathcal{X}_1 \times \mathcal{X}_2, W_{Z_1,Z_2,Z|X_1,X_2}, \mathcal{Z}_1 \times \mathcal{Z}_2 \times \mathcal{Z})$ *if there exists a sequence of* $(2^{nR_1}, 2^{nR_2}, n)$ *codes with increasing block length such that* $\lim_{n\to\infty} \mathbb{D}(P_{Z^n} || Q_Z^{\otimes n}) = 0$. *The MAC resolvability region is the closure of the set of achievable rate pairs* (R_1, R_2).

We present two achievable resolvability rate regions. In the first coding scheme, we use a block-Markov encoding that handles the causality constraint imposed by the feedback channel through careful randomness recycling to break the dependence across blocks. In the second coding scheme, a block-Markov encoding is also used. Furthermore, we harness the randomness that stems from the channel noise.

Proposition 1. *For the discrete memoryless MAC channel with generalized feedback, the following*

region is achievable via decode-and-forward if there exists a joint distribution $P_{U,X_1,X_2,Z_1,Z_2,Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z_1,Z_2,Z|X_1,X_2}$ *with marginal* Q_Z *satisfying* $I(X_1;Z_1|X_2,U) + I(X_2;Z_2|X_1,U) > I(X_1,X_2;Z)$ *for which:*

$$\begin{aligned} R_1 &\geqslant I(X_1,X_2;Z) - I(X_2;Z_1|X_1,U), \\ R_2 &\geqslant I(X_1,X_2;Z) - I(X_1;Z_2|X_2,U), \\ R_1+R_2 &\geqslant I(X_1,X_2;Z). \end{aligned}$$

Proof. We only provide a sketch of the proof. This achievable bound on the channel resolvability is constructed by allowing the two encoders to cooperate over multiple blocks. Each encoder recovers the other's message over a secure channel, i.e., the two encoders exchange information in such a way so that the output Z is oblivious to it. This is accomplished through two mechanisms: first, the feedback outputs Z_1 and Z_2 are different from the output Z, which creates a virtual wiretap channel allowing the feedback to carry information that is not accessible to Z. Second, the resolution of information available at each encoder is better than the output, because each encoder knows its own transmission and can somewhat clean up the feedback to get access to the communication from the other user.

It is interesting to note that this second mechanism was not helpful in the case of simple output feedback, also called Shannon feedback, since it was shown that feedback does not improve the resolvability rate. In the case of generalized feedback, conditioning on each encoder's own message, while decoding the feedback, seems to improve the resolvability rates.

The information exchanged during each time block is used in the next block to coordinate transmissions by the two users to facilitate obfuscation at Z. In the achievability proof, the security of the exchange of messages (mentioned in the previous paragraph) is used to demonstrate, via a chaining argument, the breaking of the dependence across blocks. □

Remark 4. *The achievable resolvability of the relay channel via decode-and-forward [18] can be retrieved from Proposition 1 by setting* $R_2 = 0$*,* $U = X_2$ *and* $Z_1 =$ *constant.*

Remark 5. *The achievable resolvability of the MAC with strictly-causal cribbing can be retrieved from Proposition 1 by setting* $Z_1 = X_2$ *and* $Z_2 = X_1$*.*

Proposition 2. *For the discrete memoryless MAC channel with generalized feedback, the following region is achievable via randomness extraction if there exists a joint distribution* $P_{X_1,X_2,Z_1,Z_2,Z} = P_{X_1} P_{X_2} W_{Z_1,Z_2,Z|X_1,X_2}$ *with marginal* Q_Z *for which:*

$$\begin{aligned} R_1 &\geqslant I(X_1;Z) - H(Z_1|X_1,Z), \\ R_2 &\geqslant I(X_2;Z) - H(Z_2|X_2,Z), \\ R_1+R_2 &\geqslant I(X_1,X_2;Z) - H(Z_1,Z_2|X_1,X_2,Z). \end{aligned}$$

Proof. We only provide a sketch of the proof. We divide the transmission into multiple blocks. In every block, each encoder independently generates randomness that stems from channel noise via a random binning argument. This fresh randomness is re-injected into the channel in the next block to assist in the approximation of output distribution. □

Remark 6. *Proposition 2 shows a* third *way in which generalized feedback improves the resolvability rate of MAC, and that is in providing* fresh *randomness to the inputs that are* independent of each other and of Z*. Our understanding of this mechanism is refined and focused via the earlier result that Shannon feedback does not improve the resolvability rate: we therefore conclude that only the fresh randomness that is independent of* Z *is useful in improving resolvability rates. This insight is not obvious because this recycled randomness is used only in the following time block and is re-processed through the channel.*

Remark 7. *The achievable resolvability of the relay channel via randomness extraction [18] can be retrieved from Proposition 2 by setting* $R_2 = 0$ *and* $Z_1 =$ *constant.*

Remark 8. *The achievable resolvability of the MAC channel can be retrieved from Proposition 2 by setting* $Z_1 = Z_2 =$ *constant.*

IV. Converse Proof of the MAC with Feedback

By assumption,

$$\begin{aligned} \epsilon &\geqslant \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \\ &= \mathbb{D}(P_{Z_1\ldots Z_n}||Q_Z^{\otimes n}) \\ &= \sum_{i=1}^n \mathbb{D}(P_{Z_i|Z^{i-1}}||Q_Z|P_{Z^{i-1}}) && (24) \\ &= \sum_{i=1}^n \mathbb{D}(P_{Z_i}||Q_Z) + \sum_{i=1}^n I(Z_i;Z^{i-1}) && (25) \end{aligned}$$

$$\begin{aligned} nR_1 &= H(M_1) && (26) \\ &\geqslant I(M_1;Z^n) && (27) \\ &= \sum_i I(M_1;Z_i|Z^{i-1}) && (28) \\ &\overset{(a)}{=} \sum_i I(M_1,X_{1i};Z_i|Z^{i-1}) && (29) \\ &\geqslant \sum_i I(X_{1i};Z_i|Z^{i-1}) && (30) \\ &= \sum_i I(Z^{i-1},X_{1i};Z_i) - \sum_i I(Z^{i-1};Z_i) && (31) \\ &\overset{(b)}{\geqslant} \sum_i I(U_i,X_{1i};Z_i) - \epsilon && (32) \\ &= \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}P_{Z_i}) - \epsilon && (33) \\ &= \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}Q_{Z_i}) - \sum_i \mathbb{D}(P_{Z_i}||Q_{Z_i}) - \epsilon \\ && (34) \end{aligned}$$

$$\overset{(c)}{\geqslant} \sum_i \mathbb{D}(P_{U_i,X_{1i},Z_i}||P_{U_i,X_{1i}}Q_{Z_i}) - \epsilon' \tag{35}$$

$$\overset{(d)}{\geqslant} n\mathbb{D}\left(\frac{\sum_i P_{P_{U_i,X_{1i},Z_i}}}{n}\middle|\middle|\frac{\sum_i P_{U_i,X_{1i}}}{n}Q_{Z_i}\right) - \epsilon' \tag{36}$$

$$= n\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}Q_Z) - \epsilon' \tag{37}$$

$$\overset{(e)}{\geqslant} n\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}\tilde{P}_Z) - \epsilon' \tag{38}$$

$$= nI(\tilde{U},\tilde{X}_1;\tilde{Z}) - \epsilon' \tag{39}$$

$$\geqslant nI(\tilde{X}_1;\tilde{Z}|\tilde{U}) - \epsilon' \tag{40}$$

where

(a) follows by the definition of the encoding function;
(b) follows since $\sum_i I(Z^{i-1};Z_i) \leqslant \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leqslant \epsilon$ and by setting $U_i \triangleq Z^{i-1}$;
(c) follows since $\sum_i \mathbb{D}(P_{Z_i}||Q_{Z_i}) \leqslant \epsilon$;
(d) follows by Jensen's inequality and convexity of $\mathbb{D}(\cdot||\cdot)$;
(e) follows since $\mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}Q_Z) = \mathbb{D}(\tilde{P}_{U,X_1,Z}||\tilde{P}_{U,X_1}\tilde{P}_Z) + \mathbb{D}(\tilde{P}_Z||Q_Z)$.

Similarly we obtain,

$$nR_2 \geqslant nI(\tilde{X}_2;\tilde{Z}|\tilde{U}) - \epsilon' \tag{41}$$

and

$$n(R_1+R_2) = H(M_1,M_2) \tag{42}$$

$$\geqslant I(M_1,M_2;Z^n) \tag{43}$$

$$= \sum_i I(M_1,M_2;Z_i|Z^{i-1}) \tag{44}$$

$$\overset{(a)}{=} \sum_i I(M_1,X_{1i},M_2,X_{2i};Z_i|Z^{i-1}) \tag{45}$$

$$\geqslant \sum_i I(X_{1i},X_{2i};Z_i|Z^{i-1}) \tag{46}$$

$$= \sum_i I(Z^{i-1},X_{1i},X_{2i};Z_i) - \sum_i I(Z^{i-1};Z_i) \tag{47}$$

$$\overset{(b)}{\geqslant} \sum_i I(U_i,X_{1i},X_{2i};Z_i) - \epsilon \tag{48}$$

$$\overset{(c)}{\geqslant} nI(\tilde{X}_1,\tilde{X}_2;\tilde{Z}|\tilde{U}) - \epsilon' \tag{49}$$

where

(a) follows by the definition of the encoding function;
(b) follows since $\sum_i I(Z^{i-1};Z_i) \leqslant \mathbb{D}(P_{Z^n}||Q_Z^{\otimes n}) \leqslant \epsilon$ and by setting $U_i \triangleq Z^{i-1}$;
(c) follows by repeating steps similar to (33)-(40).

The proof that $P_{U,X_1,X_2,Z} = P_U P_{X_1|U} P_{X_2|U} W_{Z|X_1,X_2}$ has been omitted for brevity.

V. Conclusion

We studied the impact of two-sided cooperation on the resolvability of the MAC. The main insight of this paper is that feedback does not improve resolvability of the MAC, which we show by providing a converse that is tight against the results of [13]. On the other hand, resolvability is improved in the cases of MAC with a common message, MAC with conferencing and MAC with generalized feedback. Two achievable resolvability rates are developed for the MAC with generalized feedback. The roles of decoding and randomness extraction are investigated separately. The first inner bound is constructed by using decode-and-forward strategy, where each encoder decodes the other encoder's message. The second inner bound is constructed by a randomness extraction mechanism which can be motivated by a case when each encoder's observation is very noisy, allowing cooperation without decoding.

References

[1] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[2] A. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inform. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[3] P. Cuff, "Distributed channel synthesis," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.

[4] J. Hou and G. Kramer, "Informational divergence approximations to product distributions," in *13th Canadian Workshop on Information Theory*, Toronto, ON, Canada, Jun. 2013, pp. 76–81.

[5] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1562–1575, April 2006.

[6] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inform. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.

[7] Z. Wang, R. F. Schaefer, M. Skoglund, M. Xiao, and H. V. Poor, "Strong secrecy for interference channels based on channel resolvability," *IEEE Trans. Inform. Theory*, vol. 64, no. 7, pp. 5110–5130, Jul. 2018.

[8] Z. Goldfeld, G. Kramer, H. H. Permuter, and P. Cuff, "Strong secrecy for cooperative broadcast channels," *IEEE Trans. Inform. Theory*, vol. 63, no. 1, pp. 469–495, Jan. 2017.

[9] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inform. Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[10] Y. Steinberg and S. Verdú, "Channel simulation and coding with side information," *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 634–646, May 1994.

[11] ——, "Simulation of random processes and rate-distortion theory," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 63–86, Jan. 1996.

[12] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Trans. Inform. Theory*, vol. 44, no. 2, pp. 472–487, Mar. 1998.

[13] M. Frey, I. Bjelaković, and S. Stańczak, "The MAC resolvability region, semantic security and its operational implications," arXiv preprint: 1710.02342, 2017.

[14] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *IEEE Information Theory Workshop (ITW)*, 2010, pp. 1–5.

[15] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security.*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[16] N. Helal, M. Bloch, and A. Nosratinia, "Multiple-access channel resolvability with cribbing," in *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2018, pp. 2052–2056.

[17] F. Willems and E. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," *IEEE Trans. Inform. Theory*, vol. 31, no. 3, pp. 313–327, May 1985.

[18] N. Helal, M. Bloch, and A. Nosratinia, "Channel resolvability with a full-duplex decode-and-forward relay," in *IEEE Information Theory Workshop (ITW)*, Aug. 2019.

[19] M. Bloch, "Channel intrinsic randomness," in *IEEE International Symposium on Information Theory (ISIT)*, Jun. 2010, pp. 2607–2611.

[20] N. Helal, M. Bloch, and A. Nosratinia, "Cooperative resolvability and secrecy in the cribbing multiple-access channel," arXiv preprint: 1811.11649, 2018.

[21] F. Willems, "The discrete memoryless multiple access channel with partially cooperating encoders (corresp.)," *IEEE Trans. Inform. Theory*, vol. 29, no. 3, pp. 441–445, May 1983.