Converse Coding Theorems for Identification via Multiple Access Channels

Yasutada Oohama
Department of Communication Engineering and Informatics
University of Electro-Communications
Tokyo, Japan
Email: oohama@uec.ac.jp

***Abstract*—In this paper we consider the identification (ID) via multiple access channels (MACs). In the general MAC the ID capacity region includes the ordinary transmission (TR) capacity region. In this paper we discuss the converse coding theorem. We estimate two types of error probabilities of identification for rates outside capacity region, deriving some function which serves as a lower bound of the sum of two error probabilities of identification. This function has a property that it tends to zero as $n \to \infty$ for noisy channels satisfying the strong converse property. Using this property, we establish that the transmission capacity region is equal to the ID capacity for the MAC satisfying the strong converse property. To derive the result we introduce a new resolvability problem on the output from the MAC. We further develop a new method of converting the direct coding theorem for the above MAC resolvability problem into the converse coding theorem for the ID via MACs.**

I. Introduction

In 1989, Ahlswede and Dueck [1],[2], proposed a new framework of communication system using noisy channels. Their proposed framework called the identification via channels (or briefly say the ID channel) has opened a new and fertile area in the Shannon theory. After their pioneering work, the ID channel coding problem has intensively been studied from both theoretical and practical point of view ([3]-[13]). Identification via multi-way channels is an interesting problem. This problem was studied by [6], [8], [15], [16], [17].

In this paper we deal with the identification via multiple access channels (MACs) for general noisy channels with two inputs and one output finite sets and channel transition probabilities that may be arbitrary for every block length n. Steinberg [8], and the author studied the identification(ID) capacity region for general MACs. However, these works have a common gap in the proofs of the converse coding theorems. This gap was pointed out by Hayashi [12] and is not resolved yet.

According to Steinberg [8], by a similar argument to the case of single user channels we can show that the ID capacity region contains the transmission(TR) capacity region for the general MAC. He studied the converse coding theorem by using a lemma used to prove the converse coding theorem for the ID via single user channels. In this paper we focus on our attention to the converse coding theorem and study it by an approach different from that of Steinberg. We estimate two types of error probabilities of identification for rates outside capacity region, deriving some function which serves as a lower bound of the sum of two error probabilities of identification. This function has a property that it tends to zero as $n \to \infty$ for noisy channels satisfying the strong converse property. Using this property, we establish that the transmission capacity region is equal to the ID capacity for the MAC satisfying the strong converse property.

To derive the converse coding theorem for the ID channel Han and Verdú [4] introduced an approximation problem of output distributions from single user channels. They call this problem channel resolvability problem. They first proved a direct coding theorem for the channel coding theorem and next proved a converse coding theorem for the ID channel by converting the direct coding theorem for the channel resolvability problem into the converse coding theorem for the ID channel. To prove the converse coding theorem for the ID via MACs, we formulate a new approximation problem of output distributions from MACs. This problem is regard as a MAC resolvability problem. A similar resolvability problem using MACs was studied by Steinberg [18]. Our problem is some variant of his problem. We first establish a stronger result on the direct coding theorem for this problem by deriving an upper bound for the approximation error of channel outputs to tend to zero as n goes to infinity. Next, we prove the converse coding theorem by converting the direct coding theorem for the MAC resolvability problem into the converse coding theorem for the ID via MACs.

II. Identification via Multiple Access Channels

Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be finite sets. Let $\mathcal{P}(\mathcal{X}^n)$ and $\mathcal{P}(\mathcal{Y}^n)$ be sets of probability distributions on $\mathcal{X}^n$ and $\mathcal{Y}^n$, respectively. A source $\boldsymbol{X}$ with alphabet $\mathcal{X}$ is the sequence $\{P_X^n : P_X^n \in \mathcal{P}(\mathcal{X}^n)\}_{n=1}^{\infty}$ and a source $\boldsymbol{Y}$ with alphabet $\mathcal{Y}$ is the sequence $\{P_Y^n : P_Y^n \in \mathcal{P}(\mathcal{Y}^n)\}_{n=1}^{\infty}$. Similarly, a noisy channel $\boldsymbol{W}$ with two inputs alphabets $\mathcal{X}$ and $\mathcal{Y}$ and one output alphabet $\mathcal{Z}$ is a sequence of conditional distributions $\{W^n(\cdot|\cdot,\cdot)\}_{n=1}^{\infty}$, where $W^n(\cdot|\cdot,\cdot) = \{\, W^n(\cdot|\boldsymbol{x},\boldsymbol{y}) \in \mathcal{P}(\mathcal{Z}^n)\,\}_{(\boldsymbol{x},\boldsymbol{y})\in\mathcal{X}^n\times\mathcal{Y}^n}$. Next, for $P_{X^n} \in \mathcal{P}(\mathcal{X}^n)$, $P_{Y^n} \in \mathcal{P}(\mathcal{Y}^n)$ and $\boldsymbol{z} \in \mathcal{Z}^n$, set

$$P_{X^n}P_{Y^n}W^n(\boldsymbol{z}) = \sum_{(\boldsymbol{x},\boldsymbol{y})\in\mathcal{X}^n\times\mathcal{Y}^n} P_{X^n}(\boldsymbol{x})P_{Y^n}(\boldsymbol{y})W^n(\boldsymbol{z}|\boldsymbol{x},\boldsymbol{y})\,, \quad (1)$$

which becomes a probability distribution on $\mathcal{Z}^n$. We denote it by $P_{X^n}P_{Y^n}W^n = \{P_{X^n}P_{Y^n}\ W^n(\boldsymbol{z})\ \}_{\boldsymbol{z}\in\mathcal{Z}^n}$. Set

$P_{Z^n} = P_{X^n} P_{Y^n} W^n$ and call P_{Z^n} *the response of* (P_{X^n}, P_{Y^n}) *through noisy channel* W^n *(or briefly the response of* (P_{X^n}, P_{Y^n})*).*

An $(n, N_1, N_2, \mu_n, \lambda_n)$ ID code for W^n is a collection $\{(P_{X^n|i}, P_{Y^n|j},\ D_{i,j}),\ i = 1, 2, \cdots, N_1,\ j = 1, 2, \cdots, N_2\}$ such that

1) $P_{X^n|i} \in \mathcal{P}(\mathcal{X}^n)\,, P_{Y^n|j} \in \mathcal{P}(\mathcal{Y}^n)\,,$
2) $D_{i,j} \subseteq \mathcal{Z}^n\,,$
3) $P_{Z^n|i,j}$ is the response of $(P_{X^n|i}, P_{Y^n|j})\,,$
4) $\mu_{n,ij} = P_{Z^n|i,j}(D^c_{i,j})\,, \mu_n = \max\limits_{\substack{1\le i\le N_1,\\ 1\le j\le N_2}} \mu_{n,ij}\,,$
5) $\lambda_{n,ij} = \max\limits_{(k,l)\neq(i,j)} P_{Z^n|k,l}(D_{i,j})\,, \lambda_n = \max\limits_{\substack{1\le i\le N_1,\\ 1\le j\le N_2}} \lambda_{n,ij}\,.$

The rate of an $(n, N_1, N_2, \mu_n, \lambda_n)$ ID code is defined by

$$r_{i,n} \triangleq \frac{1}{n}\log\log N_i\,, i = 1, 2.$$

A rate pair (R_1, R_2) is said to be (μ, λ)-achievable ID rate pair if there exists an $(n, N_1,\ N_2,\ \mu_n,\ \lambda_n)$ code such that

$$\left.\begin{array}{l} \limsup\limits_{n\to\infty} \mu_n \le \mu\,, \limsup\limits_{n\to\infty} \lambda_n \le \lambda\,, \\ \liminf\limits_{n\to\infty} r_{i,n} \ge R_i\,, i = 1, 2\,. \end{array}\right\}$$

The set of all (μ, λ)-achievable ID rate pairs for $\boldsymbol{W}$ is denoted by $\mathcal{C}_{\rm ID}(\mu, \lambda|\boldsymbol{W})$, which we call the (μ, λ)-ID capacity region.

To state results for the identification capacity region, we prepare several quantities which are defined based on the notion of the *information spectrum* introduced by Han and Verdú [4].

Definition 1: For $n = 1, 2, \cdots$, let X^n and Y^n be an arbitrary prescribed independent random variable taking values in $\mathcal{X}^n$ and $\mathcal{Y}^n$, respectively. The probability mass function of X^n and Y^n is $P_{X^n}(\boldsymbol{x})$, $\boldsymbol{x} \in \mathcal{X}^n$ and $P_{Y^n}(\boldsymbol{x})$, $\boldsymbol{y} \in \mathcal{Y}^n$, respectively. A pair of two independent sources $(\boldsymbol{X}, \boldsymbol{Y})$ with alphabet $\mathcal{X}\times\mathcal{Y}$ is the sequence $\{(P_{X^n}, P_{Y^n}) : P_{X^n} \in \mathcal{P}(\mathcal{X}^n),$ $P_{Y^n} \in \mathcal{P}(\mathcal{Y}^n)\}$. A collection of such $(\boldsymbol{X}, \boldsymbol{Y})$ is denoted by $\mathcal{S}_I$. Let Z^n be an output random variable when we use X^n and Y^n as two inputs of the noisy channel W^n. In this case the joint probability mass function of (X^n, Y^n, Z^n) denoted by $P_{X^nY^nZ^n}(\boldsymbol{x}, \boldsymbol{y},\ \boldsymbol{z})$, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is equal to $P_{X^n}(\boldsymbol{x})P_{Y^n}(\boldsymbol{y})\ W^n(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{y})$.

Definition 2: Given a joint distribution $P_{X^nY^nZ^n}(\ \boldsymbol{x},\ \boldsymbol{y},$ $\boldsymbol{z}) = P_{X^n}(\boldsymbol{x})P_{Y^n}(\boldsymbol{y})\ W^n(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{y})$, the information density is the function defined on $\mathcal{X}^n \times \mathcal{Y}^n$:

$$\begin{aligned} i_{X^nY^nZ^n}(\boldsymbol{x}; \boldsymbol{z}|\boldsymbol{y}) &= \log\frac{W^n(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{y})}{P_{Z^n|Y^n}(\boldsymbol{z}|\boldsymbol{y})}\,, \\ i_{X^nY^nZ^n}(\boldsymbol{y}; \boldsymbol{z}|\boldsymbol{x}) &= \log\frac{W^n(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{y})}{P_{Z^n|X^n}(\boldsymbol{z}|\boldsymbol{x})}\,, \\ i_{X^nY^nZ^n}(\boldsymbol{x}\boldsymbol{y}; \boldsymbol{z}) &= \log\frac{W^n(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{y})}{P_{Z^n}(\boldsymbol{z})}\,. \end{aligned}$$

Definition 3: Let $\{A_n\}_{n=1}^\infty$ be a sequence of arbitrary real-valued random variables. We introduce the notion of the so-called *probabilistic limsup/inf* in the following.

$$\begin{aligned} \text{p-}\limsup_{n\to\infty} A_n &\triangleq \inf\{\alpha : \lim_{n\to\infty} \Pr\{A_n \ge \alpha\} = 0\}\,, \\ \text{p-}\liminf_{n\to\infty} A_n &\triangleq \sup\{\alpha : \lim_{n\to\infty} \Pr\{A_n \le \alpha\} = 0\}\,. \end{aligned}$$

The *probabilistic limsup/inf* in the above definitions is considered as an extension of ordinary (deterministic) liminf. The operation of limsup/inf has the same properties as those of the operation of limsup/inf. For the details see Han and Verdú [4] and Han [9].

Definition 4: Set

$$\begin{aligned} \underline{I}(\boldsymbol{X}; \boldsymbol{Z}|\boldsymbol{Y}) &\triangleq \text{p-}\liminf \frac{1}{n} i_{X^nY^nZ^n}(X^n; Z^n|Y^n), \\ \underline{I}(\boldsymbol{Y}; \boldsymbol{Z}|\boldsymbol{X}) &\triangleq \text{p-}\liminf \frac{1}{n} i_{X^nY^nZ^n}(Y^n; Z^n|X^n), \\ \underline{I}(\boldsymbol{X}\boldsymbol{Y}; \boldsymbol{Z}) &\triangleq \text{p-}\liminf \frac{1}{n} i_{X^nY^nZ^n}(X^nY^n; Z^n), \\ \underline{\mathcal{C}}(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{W}) &\triangleq \{(R_1, R_2) :\ R_1 \le \underline{I}(\boldsymbol{X}; \boldsymbol{Z}|\boldsymbol{Y}), \\ &\qquad\qquad\quad R_2 \le \underline{I}(\boldsymbol{Y}; \boldsymbol{Z}|\boldsymbol{X}), \\ &\qquad\qquad\quad R_1 + R_2 \le \underline{I}(\boldsymbol{X}\boldsymbol{Y}; \boldsymbol{Z})\ \}\,, \\ \underline{\mathcal{C}}(\boldsymbol{W}) &\triangleq \bigcup_{(\boldsymbol{X},\boldsymbol{Y})\in\mathcal{S}_I} \underline{\mathcal{C}}(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{W}). \end{aligned}$$

Furthermore, set

$$\begin{aligned} \overline{I}(\boldsymbol{X}; \boldsymbol{Z}|\boldsymbol{Y}) &\triangleq \text{p-}\limsup \frac{1}{n} i_{X^nY^nZ^n}(X^n; Z^n|Y^n), \\ \overline{I}(\boldsymbol{Y}; \boldsymbol{Z}|\boldsymbol{X}) &\triangleq \text{p-}\liminf \frac{1}{n} i_{X^nY^nZ^n}(Y^n; Z^n|X^n), \\ \overline{I}(\boldsymbol{X}\boldsymbol{Y}; \boldsymbol{Z}) &\triangleq \text{p-}\liminf \frac{1}{n} i_{X^nY^nZ^n}(X^nY^n; Z^n), \\ \overline{\mathcal{C}}(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{W}) &\triangleq \{(R_1, R_2) :\ R_1 \le \overline{I}(\boldsymbol{X}; \boldsymbol{Z}|\boldsymbol{Y}), \\ &\qquad\qquad\quad R_2 \le \overline{I}(\boldsymbol{Y}; \boldsymbol{Z}|\boldsymbol{X}), \\ &\qquad\qquad\quad R_1 + R_2 \le \overline{I}(\boldsymbol{X}\boldsymbol{Y}; \boldsymbol{Z})\ \}\,, \\ \overline{\mathcal{C}}(\boldsymbol{W}) &\triangleq \bigcup_{(\boldsymbol{X},\boldsymbol{Y})\in\mathcal{S}_I} \overline{\mathcal{C}}(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{W}). \end{aligned}$$

Identification via multiple access channels was first investigated by Steinberg [8]. His result is the following.

Theorem A (Steinberg [8]) For general noisy channel $\boldsymbol{W}$, we have $\mathcal{C}_{\rm ID}(0, 0|\boldsymbol{W}) \supseteq \underline{\mathcal{C}}(\boldsymbol{W})\,.$

The above theorem can be proved by an argument quite similar to the case of the identification via single-user channels. Steinberg [8] also studied the converse coding theorem. In [8] he established a new lemma useful to prove the converse coding theorem of the identification via single-user channels. Using this lemma and the capacity formula by Verdú [19], he obtained a result on the converse coding theomrem for the identification via MACs.

In this paper we study the converse coding theorem for the ID via general MACs. Our approach is different from that of Steinberg [8]. We derive a function which serves as an upper bound of $1 - \mu_n - \lambda_n$ for general MACs. To obtain this result we formulate a new resolvability problem for the general MAC, that is, an approximation problem of output random variables via MACs. We consider this problem and derive an upper bound of the approximation error. This upper bound is useful for analyzing the error probability of identification outside the ID capacity region.

III. Main Results

A. Definitions of Functions and their Properties

We first define several functions to describe our results and state their basic properties.

Definition 5: Let S be an arbitrary subset of $\mathcal{X}^n\times \mathcal{Y}^n\times \mathcal{Z}^n$ and $\mathbf{1}_S(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})$ be indicator functions which takes value one on S and zero outside S. Set

$$\begin{aligned}
\zeta_{n,1,S} &= \zeta_{n,1,S}(R_1,P_{X^n},P_{Y^n}|W^n)\\
&= \mathsf{E}\Big[\mathrm{e}^{-n[R_1-\frac{1}{n}i_{X^nY^nZ^n}(X^n;Z^n|Y^n)]}\\
&\qquad\qquad \times \mathbf{1}_S(X^n,Y^n,Z^n)\Big],\\
\zeta_{n,2,S} &= \zeta_{n,2,S}(R_2,P_{X^n},P_{Y^n}|W^n)\\
&= \mathsf{E}\Big[\mathrm{e}^{-n[R_2-\frac{1}{n}i_{X^nY^nZ^n}(Y^n;Z^n|X^n)]}\\
&\qquad\qquad \times \mathbf{1}_S(X^n,Y^n,Z^n)\Big],\\
\zeta_{n,3,S} &= \zeta_{n,3,S}(R_1,R_2,P_{X^n},P_{Y^n},W^n)\\
&= \mathsf{E}\Big[\Big\{\mathrm{e}^{-n[R_1-\frac{1}{n}i_{X^nZ^n}(X^n;Z^n)]}\\
&\qquad +\mathrm{e}^{-n[R_2-\frac{1}{n}i_{Y^nZ^n}(Y^n;Z^n)]}\\
&\qquad +\mathrm{e}^{-n[R_1+R_2-\frac{1}{n}i_{X^nY^nZ^n}(X^nY^n;Z^n)]}\Big\}\\
&\qquad\qquad \times \mathbf{1}_S(X^n,Y^n,Z^n)\Big].
\end{aligned}$$

Definition 6: Set

$$\begin{aligned}
T_\gamma = \{\, &(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\in \mathcal{X}^n\times\mathcal{Y}^n\times\mathcal{Z}^n :\\
&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{x};\boldsymbol{z}|\boldsymbol{y})\le R_1-\gamma\,,\\
\text{or }&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{y};\boldsymbol{z}|\boldsymbol{x})\le R_2-\gamma\,,\\
\text{or }&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{x}\boldsymbol{y};\boldsymbol{z})\le R_1+R_2-2\gamma\,\}\,.
\end{aligned}$$

Define three subsets of $\mathcal{X}^n\times\mathcal{Y}^n\times\mathcal{Z}^n$ by

$$\begin{aligned}
T_{1,\gamma} = \{\, &(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\in \mathcal{X}^n\times\mathcal{Y}^n\times\mathcal{Z}^n :\\
&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{x};\boldsymbol{z}|\boldsymbol{y})\le R_1-\gamma\,\}\,,\\
T_{2,\gamma} = \{\, &(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\in \mathcal{X}^n\times\mathcal{Y}^n\times\mathcal{Z}^n :\\
&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{y};\boldsymbol{z}|\boldsymbol{x})\le R_2-\gamma\,\}\,,\\
T_{3,\gamma} = \{\, &(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})\in \mathcal{X}^n\times\mathcal{Y}^n\times\mathcal{Z}^n :\\
&\frac{1}{n}i_{X^nZ^n}(\boldsymbol{x};\boldsymbol{z})\le R_1-\gamma\,,\\
&\frac{1}{n}i_{Y^nZ^n}(\boldsymbol{y};\boldsymbol{z})\le R_2-\gamma\,,\\
&\frac{1}{n}i_{X^nY^nZ^n}(\boldsymbol{x}\boldsymbol{y};\boldsymbol{z})\le R_1+R_2-2\gamma\,\}\,.
\end{aligned}$$

Set

$$\begin{aligned}
&\Omega^{(1)}_{n,i,\gamma}(R_i,P_{X^n},P_{Y^n}|W^n)\\
&= \Pr\{(X^n,Y^n,Z^n)\notin T_{i,\gamma}\}\,, i=1,2,\\
&\Omega^{(1)}_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\\
&= \Pr\{(X^n,Y^n,Z^n)\notin T_{3,\gamma}\}\,,\\
&\Omega^{(2)}_{n,i,\gamma}(R_i,P_{X^n},P_{Y^n}|W^n)\\
&= \zeta_{n,i,T_{i,\gamma}}(R_i,P_{X^n},P_{Y^n}|W^n), i=1,2,\\
&\Omega^{(2)}_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\\
&= \zeta_{n,3,T_{3,\gamma}}(R_1,R_2,P_{X^n},P_{Y^n}|W^n),\\
&\Omega_{n,i,\gamma}(R_i,P_{X^n},P_{Y^n}|W^n)\\
&= 4\Omega^{(1)}_{n,i,\gamma}(R_i,P_{X^n},P_{Y^n}|W^n)\\
&\qquad +3\sqrt{\Omega^{(2)}_{n,i,\gamma}(R_i,P_{X^n},P_{Y^n}|W^n)}, i=1,2,\\
&\Omega_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\\
&= 4\Omega^{(1)}_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\\
&\qquad +3\sqrt{\Omega^{(2)}_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)}.
\end{aligned}$$

Furthermore, set

$$\begin{aligned}
&\Omega_{n,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\\
&\quad = \min\{\Omega_{n,1,\gamma}(R_1,P_{X^n},P_{Y^n}|W^n),\\
&\qquad\quad \Omega_{n,2,\gamma}(R_2,P_{X^n},P_{Y^n}|W^n),\\
&\qquad\quad \Omega_{n,3,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\}
\end{aligned}$$

Finally, set

$$\begin{aligned}
&\Omega_{n,\gamma}(R_1,R_2|W^n)\\
&= \sup_{\substack{(P_{X^n},P_{Y^n})\\ \in\mathcal{P}(\mathcal{X}^n)\times\mathcal{P}(\mathcal{Y}^n)}} \Omega_{n,\gamma}(R_1,R_2,P_{X^n},P_{Y^n}|W^n)\,. \qquad (2)
\end{aligned}$$

We can prove that $\Omega_{n,\gamma}(\,R_1,R_2,\,W^n)$ satisfies the following property.

Property 1:

a) For any $\gamma\ge 0$ and $R_1,R_2\ge 0$,

$$0\le \Omega_{n,\gamma}(R_1,R_2,W^n)\le \frac{73}{16}\,.$$

b) Set

$$\begin{aligned}
&\overline{\mathcal{C}}'(\boldsymbol{X},\boldsymbol{Y}|\boldsymbol{W})\\
&\stackrel{\triangle}{=} \overline{\mathcal{C}}(\boldsymbol{X},\boldsymbol{Y}|\boldsymbol{W})\\
&\quad \cup\{(R_1,R_2): R_1\le \overline{I}(\boldsymbol{X};\boldsymbol{Z}), R_2\le \overline{I}(\boldsymbol{Y};\boldsymbol{Z}|\boldsymbol{X})\}\\
&\quad \cup\{(R_1,R_2): R_1\le \overline{I}(\boldsymbol{X};\boldsymbol{Z}|\boldsymbol{Y}), R_2\le \overline{I}(\boldsymbol{Y};\boldsymbol{Z})\},\\
&\overline{\mathcal{C}}'(\boldsymbol{W}) \stackrel{\triangle}{=} \bigcup_{(\boldsymbol{X},\boldsymbol{Y})\in\mathcal{S}_I} \overline{\mathcal{C}}'(\boldsymbol{X},\boldsymbol{Y}|\boldsymbol{W}).
\end{aligned}$$

It is obvious that $\overline{\mathcal{C}}(\boldsymbol{W})\subseteq\overline{\mathcal{C}}'(\boldsymbol{W})$. If $(R_1,R_2)\notin\overline{\mathcal{C}}'(\boldsymbol{W})$, then, there exists a small positive number γ_0 such that for any $\gamma\in[0,\gamma_0)$,

$$\lim_{n\to\infty}\Omega_{n,\gamma}(R_1,R_2|W^n)=0.$$

Proof of Property 1 part a) is quite parallel with that of Property 2 part a) in [13]. Proof of Property 1 part b) is found in the appendix in [14].

B. Statement of Results

Our main result for the identification via MACs is the following.

Proposition 1: For any $(n, N_1, N_2, \mu_n, \lambda_n)$ code with $\mu_n + \lambda_n < 1$, if the rate $r_{i,n} = \frac{1}{n}\log\log N_i$ satisfies

$$r_{1,n} \geq R_1 + \frac{\log n}{n} + \frac{1}{n}\log\log(3|\mathcal{X}|)^2\,, \tag{3}$$

$$r_{2,n} \geq R_2 + \frac{\log n}{n} + \frac{1}{n}\log\log(3|\mathcal{Y}|)^2\,, \tag{4}$$

then, for any $\gamma \geq 0$, the sum $\mu_n + \lambda_n$ of two error probabilities satisfies the following:

$$1 - \mu_n - \lambda_n \leq \Omega_{n,\gamma}(R_1, R_2|W^n)\,.$$

From Theorem A, Proposition 1, and Property 1 part b), the following strong converse theorem holds.

Theorem 1: For any sequence of ID codes $\{(n, N_1, N_2, \mu_n, \lambda_n)\}_{n=1}^{\infty}$ satisfying $\mu_n + \lambda_n < 1$, $n = 1, 2, \cdots$, if

$$\liminf_{n\to\infty} r_{i,n} \geq R_i, i = 1, 2, \quad (R_1, R_2) \notin \overline{\mathcal{C}}'(\boldsymbol{W})\,,$$

then,

$$\liminf_{n\to\infty}\{\mu_n + \lambda_n\} = 1,$$

which implies that for any $\mu \geq 0, \lambda \geq 0$, $\mu + \lambda < 1$ and any noisy channel $\boldsymbol{W}$,

$$\underline{\mathcal{C}}(\boldsymbol{W}) \subseteq \mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W}) \subseteq \overline{\mathcal{C}}'(\boldsymbol{W})\,.$$

In particular, if $\underline{\mathcal{C}}(\boldsymbol{W}) = \overline{\mathcal{C}}'(\boldsymbol{W})$, then, for any $\mu \geq 0, \lambda \geq 0$, $\mu + \lambda < 1$,

$$\underline{\mathcal{C}}(\boldsymbol{W}) = \mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W}) = \overline{\mathcal{C}}'(\boldsymbol{W}).$$

Furthermore, $\mu_n + \lambda_n$ converges to one as $n \to \infty$ at rates above the ID capacity. This implies that the strong converse property holds with respect to the sum of two types of error probabilities.

C. Results for the Average Error Criterion

We have so far dealt with the case that the error probabilities of identification are measured in the maximum sense. In this subsection we consider the following average error criterion:

$$\left.\begin{aligned} \bar{\mu}_n &= \frac{1}{N_1 N_2}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}\mu_{n,ij}\,, \\ \bar{\lambda}_n &= \frac{1}{N_1 N_2}\sum_{i=1}^{N_1}\sum_{j=1}^{N_2}\lambda_{n,ij}\,. \end{aligned}\right\} \tag{5}$$

For $0 \leq \mu, \lambda \leq 1$, let $\mathcal{C}_{\mathrm{ID,a}}(\mu, \lambda|\boldsymbol{W})$ be denoted by the identification capacity defined by replacing the maximum error probability criterion by the above average error probability criterion. Since $\bar{\mu}_n \leq \mu_n$ and $\bar{\lambda}_n \leq \lambda_n$, it is obvious that for any $\mu, \lambda \geq 0$,

$$\mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W}) \subseteq \mathcal{C}_{\mathrm{ID,a}}(\mu, \lambda|\boldsymbol{W})\,. \tag{6}$$

We shall show that $\mathcal{C}_{\mathrm{ID,a}}(\mu, \lambda|\boldsymbol{W})$ has the same outer bound as $\mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W})$. An important key result in the case of the average error criterion is given in the following proposition.

Proposition 2: Fix $\tau > 0$ arbitrarily. For any $(n, N_1, N_2, \bar{\mu}_n, \bar{\lambda}_n)$ code with $\bar{\mu}_n + \bar{\lambda}_n < 1$ if the rate $r_{i,n} = \frac{1}{n}\log\log N_i$, $i = 1, 2$ satisfy

$$r_{1,n} \geq R_1 + \tau + \frac{\log n}{n} + \frac{1}{n}\log\log|\mathcal{X}|^2\,, \tag{7}$$

$$r_{2,n} \geq R_2 + \tau + \frac{\log n}{n} + \frac{1}{n}\log\log|\mathcal{Y}|^2\,, \tag{8}$$

then, for any $\gamma \geq 0$, the sum $\bar{\mu}_n + \bar{\lambda}_n$ of two average error probabilities satisfies the following:

$$\begin{aligned} 1 - \bar{\mu}_n - \bar{\lambda}_n \leq{}& \Omega_{n,\gamma}(R_1, R_2|W^n) \\ &+ \nu_{n,\tau}(R_1, R_2, |\mathcal{X}|, |\mathcal{Y}|), \end{aligned}$$

where

$$\begin{aligned} &\nu_{n,\tau}(R_1, R_2, |\mathcal{X}|, |\mathcal{Y}|) \\ &\triangleq |\mathcal{X}|^{-2n(\mathrm{e}^{n\tau}-1)\mathrm{e}^{nR_1}}|\mathcal{Y}|^{-2n(\mathrm{e}^{n\tau}-1)\mathrm{e}^{nR_2}} \\ &\quad+|\mathcal{X}|^{-2n(\mathrm{e}^{n\tau}-1)\mathrm{e}^{nR_1}}\cdot|\mathcal{Y}|^{-2n(\mathrm{e}^{n\tau}-1)\mathrm{e}^{nR_2}}. \end{aligned}$$

Since $\mathrm{e}^{n\tau} - 1 \geq n\tau$, we have

$$\begin{aligned} 0 &\leq \nu_{n,\tau}(R_1, R_2, |\mathcal{X}|, |\mathcal{Y}|) \\ &\leq |\mathcal{X}|^{-2n^2\tau\mathrm{e}^{nR_1}} + |\mathcal{Y}|^{-2n^2\tau\mathrm{e}^{nR_2}} \\ &\quad+|\mathcal{X}|^{-2n^2\tau\mathrm{e}^{nR_1}}\cdot|\mathcal{Y}|^{-2n^2\tau\mathrm{e}^{nR_2}} \\ &\leq 3|\mathcal{X}|^{-2n^2\tau\mathrm{e}^{nR_1}}\cdot|\mathcal{Y}|^{-2n^2\tau\mathrm{e}^{nR_2}}, \end{aligned}$$

which implies that for each fixed $\tau > 0$, $\nu_{n,\tau}(R_1, R_2, |\mathcal{X}|, |\mathcal{Y}|)$ decays double exponentially as n tends to infinity.

From Theorem A, Proposition 2, and Property 1 part b), the following strong converse theorem holds.

Theorem 2: For any sequence of ID codes $\{(n, N_1, N_2, \bar{\mu}_n, \bar{\lambda}_n)\}_{n=1}^{\infty}$ satisfying $\bar{\mu}_n + \bar{\lambda}_n < 1$, $n = 1, 2, \cdots$, if

$$\liminf_{n\to\infty} r_{i,n} \geq R_i, i = 1, 2, \quad (R_1, R_2) \notin \overline{\mathcal{C}}'(\boldsymbol{W})\,,$$

then,

$$\liminf_{n\to\infty}\{\bar{\mu}_n + \bar{\lambda}_n\} = 1,$$

which implies that for any $\mu \geq 0, \lambda \geq 0$, $\mu + \lambda < 1$ and any noisy channel $\boldsymbol{W}$,

$$\underline{\mathcal{C}}(\boldsymbol{W}) \subseteq \mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W}) \subseteq \mathcal{C}_{\mathrm{ID,a}}(\mu, \lambda|\boldsymbol{W}) \subseteq \overline{\mathcal{C}}'(\boldsymbol{W})\,.$$

In particular, if $\underline{\mathcal{C}}(\boldsymbol{W}) = \overline{\mathcal{C}}'(\boldsymbol{W})$, then, for any $\mu \geq 0, \lambda \geq 0$, $\mu + \lambda < 1$,

$$\underline{\mathcal{C}}(\boldsymbol{W}) = \mathcal{C}_{\mathrm{ID}}(\mu, \lambda|\boldsymbol{W}) = \mathcal{C}_{\mathrm{ID,a}}(\mu, \lambda|\boldsymbol{W}) = \overline{\mathcal{C}}'(\boldsymbol{W})\,.$$

Furthermore, $\bar{\mu}_n + \bar{\lambda}_n$ converges to one as $n \to \infty$ at rates above the ID capacity. This implies that the strong converse property holds with respect to the sum of two types of error probabilities.

IV. Outline of Proofs of the Results

In this section we shall give outline of the proofs of Propositions 1 and 2. For the proofs of those two propositions we formulate a new resolvability problem for the general MAC, that is, an approximation problem of output random variables via MACs. We consider this problem and derive an upper bound of the approximation error. This upper bound is useful for analyzing the error probability of identification outside the ID capacity region.

Definition 7: Let $U_{M_i}, i = 1, 2$ be the uniform random variables taking values in $\mathcal{U}_{M_1} = \{1, 2, \cdots, M_i\}$. By two maps $\tilde{\varphi}_1 : \mathcal{U}_{M_1} \to \mathcal{X}^n$ and $\tilde{\varphi}_2 : \mathcal{U}_{M_2} \to \mathcal{Y}^n$, the uniform random variables U_{M_1} and U_{M_2} is transformed into the random variable $\tilde{X}^n = \tilde{\varphi}_1(U_{M_1})$ and $\tilde{Y}^n = \tilde{\varphi}_2(U_{M_2})$, respectively. Let $\mathcal{P}_{M_1}$ $(\mathcal{X}^n)$ and $\mathcal{P}_{M_2}$ $(\mathcal{Y}^n)$ be sets of all probability distributions on $\mathcal{X}^n$ that can be created by the transformation of U_{M_1} and U_{M_2}. Elements of $\mathcal{P}_{M_1}(\mathcal{X}^n)$ and $\mathcal{P}_{M_2}(\mathcal{Y}^n)$, respectively are called M_1 and M_2-types. Every random variable $\tilde{X}^n = \tilde{\varphi}_1(\ U_{M_1}\ )$ created by some transformation map $\tilde{\varphi}_1 :$ $\mathcal{U}_{M_n} \to \mathcal{X}^n$ and U_{M_1} has M_1-type. Similarly, every random variable $\tilde{Y}^n = \tilde{\varphi}_2(\ U_{M_2}\ )$ created by some transformation map $\tilde{\varphi}_2 : \mathcal{U}_{M_2} \to \mathcal{Y}^n$ and U_{M_2} has M_2-type.

Definition 8: For $\tilde{\varphi}_1 : \mathcal{U}_{M_1} \to \mathcal{X}^n$ and $\tilde{\varphi}_2 : \mathcal{U}_{M_2} \to \mathcal{Y}^n$, define $P_{\tilde{X}^n} = P_{\tilde{\varphi}_1(U_{M_1})}$ and $P_{\tilde{Y}^n} = P_{\tilde{\varphi}_2(U_{M_2})}$. We use $P_{\tilde{X}^n}$ and $P_{\tilde{Y}^n}$ as approximations of X^n and Y^n, respectively. Let $\tilde{Q}^{(1)}$ be a response of $(P_{\tilde{X}^n}, P_{Y^n})$ and let $\tilde{Q}^{(2)}$ be a response of $(P_{X^n}, P_{\tilde{Y}^n})$. Let $\tilde{Q}^{(3)}$ be a response of $(P_{\tilde{X}^n}, P_{\tilde{Y}^n})$. Set

$$\underline{\tilde{Q}} \stackrel{\triangle}{=} (\tilde{Q}^{(1)}, \tilde{Q}^{(2)}, \tilde{Q}^{(3)}).$$

Let $\tilde{\mathcal{Q}}^{(t)}$, $t = 1, 2, 3$, be sets of all responses $\tilde{Q}^{(t)}$.

Now we use $\underline{\tilde{Q}}$ as an approximation of Q. We shall derive explicit upper bounds of the three approximation errors $d(Q, \tilde{Q}^{(t)}), t = 1, 2, 3$ measured by the variational distance. This result is a mathematical core of the converse coding theorem for the ID via MACs.

Lemma 1: Set $M_t = \lceil \mathrm{e}^{nR_t} \rceil$, $t = 1, 2$, where $\lceil a \rceil$ is the minimum integer not below a. Let $S_i, i = 1, 2, 3$ be arbitrary prescribed subsets of $\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$. Let (X^n, Y^n) be a pair of two independent random variables with distribution $(P_{X^n}$, $P_{Y^n})$. Let Q be a response of $(P_{X^n},\ P_{Y^n})$. Then, for any $(P_{X^n},\ P_{Y^n})$ and its response Q, there exist $\tilde{\varphi}_1 : \mathcal{U}_{M_1} \to \mathcal{X}^n$ and $\tilde{\varphi}_2 : \mathcal{U}_{M_2} \to \mathcal{Y}^n$ such that the three variational distances $d(Q, \tilde{Q}^{(t)})$, $t = 1, 2, 3$ satisfies the following:

$$\begin{aligned} & d(Q, \tilde{Q}^{(t)}) \\ & \leq 4\mathsf{E}\left[\mathbf{1}_{S_t^c}(X^n, Y^n, Z^n)\right] + 3\sqrt{\zeta_{n,t,S_t}}. \end{aligned}$$

The proof of the above lemma is given in appendix in [14]. This lemma is useful for the proofs of Propositions 1 and 2. Approximation problem of the output distribution Q using $\tilde{Q}^{(3)}$ was posed and investigated by [18]. Introduction of the two approximation problems of Q using $\tilde{Q}^{(1)}$ and $\tilde{Q}^{(2)}$ is new. A combination of the three approximation problems using $\tilde{Q}^{(t)}, t = 1, 2, 3$ is essential in the proof of the converse coding theorem of the ID via MACs. For the proofs of Propositions 1 and 2 we also need a new method of converting the direct coding theorem for the MAC resolvability problem into the converse coding theorem of the ID via MACs. Han and Verdú [4] provided a method of converting the direct coding theorem for the channel resolvability problem into the converse coding theorem of the ID channel. Our method is an extension of their method in the case of MACs. The detail is found in [14].

References

[1] R. Ahlswede and G. Dueck, "Identification via channels" *IEEE Trans. Inform. Theory*, vol. 35, pp. 15-29, Jan. 1989.

[2] ____, "Identification in the presence of feedback –A discovery of new capacity formulas" *IEEE Trans. Inform. Theory*, vol. 35, pp. 30-36, Jan. 1989.

[3] T. S. Han and S. Verdú, "New results in the theory of identification via channels," *IEEE Trans. Inform. Theory*, vol. 38, pp. 14-25, Jan. 1992.

[4] ____, "Approximation theory of output statistics," *IEEE Trans. Inform. Theory*, vol. 39, pp. 752-722, May 1993.

[5] M. V. Burnashev ad S. Verdú, "Measures separated in L1 metrics and ID codes," *Probl. Inform. Transm.*, vol. 30, no. 3, pp. 191-201, 1994.

[6] R. Ahlswede and Z. Zhang, "New directions in the theory of identification via channels," *IEEE Trans. Inform. Theory* vol. 41, pp. 1040-1050, July 1995.

[7] L. A. Bassalygo and M.V. Burnashev, "Authentication, identification and pairwise separated measures," *Probl. Inform. Transm.*, vol. 32, no. 1, pp. 33-39, 1996.

[8] Y. Steinberg, "New converses in the theory of identification via channels," *IEEE Trans. Inform. Theory*, vol. 44, pp. 984-998, May 1998.

[9] T. S. Han, *Information-Spectrum Methods in Information Theory. (in Japanese)* Baifukan, Tokyo, 1998.

[10] M. V. Burnashev, "On identification capacity of infinite alphabets or continuous-time channels," *IEEE Trans. Inform. Theory* vol. 46, pp. 2407-2414, Nov. 2000.

[11] Y. Steinberg and N. Merhav, "Identification in the presence of side information with application to watermarking," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1410-1422, May 2001.

[12] M. Hayashi,"General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1562-1575, April 2006.

[13] Y. Oohama, "Converse coding theorems for identification via channels," *IEEE Trans. Inform. Theory*, vol. 59, pp. 744-759, Feb. 2013.

[14] Y. Oohama, "Outer bound of the capacity region for identification via multiple access channels,"*preprint;* available at http://arxiv.org/PS_cache.

[15] B. Verboven and E. C. van der Meulen, "Capacity bounds for identification via broad cast channels that are optimal for the deterministic broadcast channel," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1197-1205, Nov. 1990.

[16] R. Ahlswede and B. Verboven, "On identification via multiway channels with feedback," *IEEE Trans. Inform. Theory* vol. 37, pp. 1519-1526, Nov. 1991.

[17] Y. Oohama, "Converse coding theorem for the identification via multiple access channels," *IEEE Inform. Theory Workshop*, Bangalore, India, Oct. 20-25, pp. 155-158, 2002.

[18] Y. Steinberg, "Resolvability theory for the multiple-accsess channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 472-487, March 1998.

[19] S. Verdú, "Multiple-access channels with memory with and without frame synchronism," *IEEE Trans. Inform. Theory*, vol 35, pp. 605-619, May 1989.