The Identification Capacity of the Modulo-Additive Noise Channel with Help

Amos Lapidoth and Baohua Ni
Signal and Information Processing Laboratory
ETH Zurich, 8092 Zurich, Switzerland
lapidoth, baohni@isi.ee.ethz.ch

***Abstract*—The gain in the Identification Capacity afforded by a rate-limited description of the noise sequence corrupting a modulo-additive noise channel is studied. Both the classical Ahlswede-Dueck version and the Ahlswede-Cai-Ning-Zhang version, which does not allow for missed identifications, are studied. Irrespective of whether the help is provided to the transmitter, to the receiver, or to both—the two capacities coincide and both equal the helper-assisted Shannon capacity.**

I. Introduction

If a helper can observe the additive noise corrupting a channel and can describe it to the decoder, then the latter can subtract it and thus render the channel noiseless. But, for this to succeed, the description must be nearly lossless and hence possibly of formidable rate. It is thus of interest to study scenarios where the description rate is limited and to understand how the rate of the help affects performance.

When performance is measured in terms of the Shannon capacity, the problem was solved for a number of channel models in [1], [2], and [3], where the former two address assistance to the decoder and the latter to the encoder. When performance is measured in terms of the Erasures-Only capacity or the List-Size capacity, the problem was solved in [4] and [5]. Error exponents with assistance were studied in [6]. Here we study how rate-limited help affects the Identification capacity [7].

We focus on the memoryless modulo-additive channel (MMANC) whose time-k output Y_k corresponding to the time-k input x_k is

$$Y_k = x_k \oplus Z_k,$$

where Z_k is the time-k noise sample; the channel input x_k, the channel output Y_k, and the noise Z_k all take values in the set $\mathcal{A}$—also denoted $\mathcal{X}$, or $\mathcal{Y}$, or $\mathcal{Z}$—comprising the $|\mathcal{A}|$ elements $\{0, \ldots, |\mathcal{A}| - 1\}$; and $\oplus$ and $\ominus$ denote mod-$|\mathcal{A}|$ addition and subtraction respectively. The noise sequence $\{Z_k\}$ is IID $\sim P_Z$, where P_Z is some PMF on $\mathcal{A}$.

Irrespective of whether the help is provided to the encoder, to the decoder, or to both, the Shannon capacity of this channel coincides with its Erasures-Only capacity and both are given by [3, Section V] [4, Theorems 2 and 6]

$$C_{\text{e-o}}(R_{\text{h}}) = C_{\text{Sh}}(R_{\text{h}}) = \log|\mathcal{A}| - \big\{H(Q_Z) - R_{\text{h}}\big\}^+, \quad (1)$$

where $\{\xi\}^+$ denotes $\max\{0, \xi\}$, and $H(Q_Z)$ is the Shannon entropy of Q_Z.

Here we study two versions of the Identification capacity of this channel: Ahlswede and Dueck's original Identification capacity C_{ID} [7] and the Identification capacity subject to no missed-identifications $C_{\text{ID},0}$ [8]. Our main result is that—irrespective of whether the help is provided to the encoder, to the decoder, or to both—the two identification capacities coincide, and both equal the right-hand side (RHS) of (1).

II. Problem Formulation

The channel identification problem is parameterized by the blocklength n, which tends to infinity in the definition of the Identification capacity. The n-length noise sequence $Z^n \in \mathcal{A}^n$ is presented to the helper, which produces its nR_{h}-bit description $t(Z^n)$

$$t(z^n) \in \mathcal{T}$$

where

$$\mathcal{T} = \{0,1\}^{nR_{\text{h}}}.$$

We refer to the set $\mathcal{N} = \{1, \ldots, \mathsf{N}\}$ as the set of identification messages and to its cardinality N as the number of identification messages. The identification rate is defined (for N sufficiently large) as

$$\frac{1}{n}\log\log \mathsf{N}.$$

A generic element of $\mathcal{N}$—namely, a generic identification message—is denoted i.

If no help is provided to the encoder, then the latter is specified by a family $\{P^i_{X^n}\}_{i\in\mathcal{N}}$ of PMFs on $\mathcal{A}^n$ that are indexed by the identification messages, with the understanding that, to convey Identification Message (IM) i, the encoder transmits a random sequence in $\mathcal{A}^n$ that it draws according to the PMF $P^i_{X^n}$. If help $T = t(Z^n) \in \mathcal{T}$ is provided to the encoder, then the encoder's operation is specified by a family of PMFs $\{P^i_{X^n|t}\}_{(i,t)\in\mathcal{N}\times\mathcal{T}}$ that is now indexed by pairs of identification messages and noise descriptions, with the understanding that, to convey IM i given the description $T = t(Z^n)$, the encoder produces a random n-length sequence of channel inputs that is distributed according to $P^i_{X^n|T}$. In either case, the channel output sequence Y^n is

$$Y^n = X^n \oplus Z^n$$

componentwise.

978-1-6654-7554-9/23/$31.00 ©2023 IEEE

If help is provided to the encoder, and if IM i is to be conveyed, then the joint distribution of (X^n, Z^n, Y^n, T) has the form

$$P_{Z^n}(z^n)\, P_{T|Z^n}(t|z^n)\, P^i_{X^n|T}(x^n|t)\, P_{Y^n|X^n,Z^n}(y^n|x^n,z^n),$$

where[1]

$$P_{T|Z^n}(t|z^n) = \mathbb{1}\big\{t = t(z^n)\big\},$$

and

$$P_{Y^n|X^n,Z^n}(y^n|x^n,z^n) = \mathbb{1}\big\{y^n = x^n \oplus z^n\big\},$$

where $\mathbb{1}\big\{\text{Statement}\big\}$ is equal to 1 if the statement holds and is equal to 0 otherwise. In the absence of help, the joint distribution has the form

$$P_{Z^n}(z^n)\, P_{T|Z^n}(t|z^n)\, P^i_{X^n}(x^n)\, P_{Y^n|X^n,Z^n}(y^n|x^n,z^n).$$

Based on the data available to it—Y^n in the absence of help to the decoder and $(Y^n, t(Z^n))$ in its presence—the receiver performs N binary tests indexed by $i \in \mathcal{N}$, where the i-th test is whether or not the IM was i. It accepts the hypothesis that the IM was i if Y^n is in its acceptance region, which we denote $\mathcal{D}_i(t) \in \mathcal{A}^n$ in the presence of decoder assistance $t \in \mathcal{T}$ and $\mathcal{D}_i \in \mathcal{A}^n$ in its absence.

When the help $t \in \mathcal{T}$ is provided to the receiver, the probability of missed detection associated with IM i is thus

$$p^i_{\text{MD}}(t) = 1 - P^i_{Y^n|T=t}\big(\mathcal{D}_i(t)\big)$$

and the worst-case false alarm associated with IM i is

$$p^i_{\text{FA}}(t) = \max_{j \in \mathcal{N}\setminus\{i\}} P^j_{Y^n|T=t}\big(\mathcal{D}_i(t)\big).$$

Note that, given $t \in \mathcal{T}$, the acceptance regions $\{\mathcal{D}_i(t)\}_{i\in\mathcal{N}}$ of the different tests need not be disjoint. We define

$$p_{\text{MD,max}} = \max_{i\in\mathcal{N}} \sum_{t\in\mathcal{T}} P_T(t)\, p^i_{\text{MD}}(t), \tag{2}$$

and

$$p_{\text{FA,max}} = \max_{i\in\mathcal{N}} \sum_{t\in\mathcal{T}} P_T(t)\, p^i_{\text{FA}}(t). \tag{3}$$

In the absence of help to the receiver, the probability of missed detection associated with IM i is

$$p^i_{\text{MD}} = 1 - P^i_{Y^n}(\mathcal{D}_i)$$

and the worst-case probability of false alarm associated with it is

$$p^i_{\text{FA}} = \max_{j\in\mathcal{N}\setminus\{i\}} P^j_{Y^n}(\mathcal{D}_i).$$

In this case, we define

$$p_{\text{MD,max}} = \max_{i\in\mathcal{N}} p^i_{\text{MD}}$$

and

$$p_{\text{FA,max}} = \max_{i\in\mathcal{N}} p^i_{\text{FA}}.$$

In both cases we say that a scheme is of **zero missed detections** if $p_{\text{MD,max}}$ is zero.

A rate R is an achievable identification rate if, for every $\gamma > 0$ and every $\epsilon > 0$, there exists some positive integer n_0 such that, for all blocklengths n exceeding n_0, there exists a scheme with

$$\mathsf{N} = \big\lceil 2^{2^{n(R-\gamma)}} \big\rceil$$

identification messages for which

$$\max\{p_{\text{MD,max}},\, p_{\text{FA,max}}\} < \epsilon. \tag{4}$$

The supremum of achievable rates is the Identification capacity with a helper $C_{\text{ID}}(R_{\text{h}})$. Replacing the requirement (4) with

$$p_{\text{MD,max}} = 0, \qquad p_{\text{FA,max}} < \epsilon \tag{5}$$

leads to the definition of the **zero missed-identification capacity** $C_{\text{ID},0}(R_{\text{h}})$.

The following theorem is the main result of this paper.

Theorem 1: On the modulo additive noise channel—irrespective of whether the help is provided to the transmitter, to the receiver, or to both—the Identification capacity with a helper $C_{\text{ID}}(R_{\text{h}})$ and the Zero Missed-Identification capacity with a helper $C_{\text{ID},0}(R_{\text{h}})$ are equal and coincide with the Shannon capacity

$$C_{\text{ID}}(R_{\text{h}}) = C_{\text{ID},0}(R_{\text{h}}) = C_{\text{Sh}}(R_{\text{h}})$$

where the latter is given in (1).

We prove this result by establishing that $C_{\text{ID},0}(R_{\text{h}}) \geq C_{\text{Sh}}(R_{\text{h}})$ using the recent results in [4] in combination with the code construction proposed in [8]. The converse, is proved by analyzing the case where the assistance is provided to both transmitter and receiver using the techniques developed in [9].

[1] We are assuming that the noise description is a deterministic function of the noise sequence, but the results also hold if we allow randomized descriptions. In fact, our coding schemes are of deterministic descriptions and the converse allows for randomization.

References

[1] Y.-H. Kim, "Capacity of a class of deterministic relay channels," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 1328–1329, 2008.

[2] S. I. Bross, A. Lapidoth, and G. Marti, "Decoder-assisted communications over additive noise channels," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4150–4161, 2020.

[3] A. Lapidoth and G. Marti, "Encoder-assisted communications over additive noise channels," *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 6607–6616, 2020.

[4] A. Lapidoth, G. Marti, and Y. Yan, "Other helper capacities," in *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2021, pp. 1272–1277.

[5] A. Lapidoth and Y. Yan, "The listsize capacity of the Gaussian channel with decoder assistance," *Entropy*, vol. 24, no. 1, 2022. [Online]. Available: https://www.mdpi.com/1099-4300/24/1/29

[6] N. Merhav, "On error exponents of encoder-assisted communication systems," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 7019–7029, 2021.

[7] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 15–29, 1989.

[8] R. Ahlswede, N. Cai, and Z. Zhang, "Erasure, list, and detection zero-error capacities for low noise and a relation to identification," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 55–62, 1996.

[9] S. Watanabe, "Minimax converse for identification via channels," *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 25–34, 2022.