On the Zero-Error Capacity with Helper

Amos Lapidoth and Yiming Yan
ETH Zurich
8092 Zurich, Switzerland
{lapidoth, yan}@isi.ee.ethz.ch

***Abstract*—The zero-error helper capacity of the modulo-additive noise channel is studied both in the presence and in the absence of feedback. In its presence, a complete solution of said capacity is provided. In its absence, a solution is provided when the alphabet size is prime. For all other cases, a necessary and sufficient condition for positivity is provided. Thanks to the help, the zero-error capacity may increase by more than the help's rate, and it can be positive yet smaller than one bit.**

I. Introduction

This paper investigates the extent to which the zero-error capacity can benefit from a rate-limited description of the noise. We study both encoder assistance, where the description is provided to the encoder before transmission begins, and decoder assistance, where it is provided to the decoder. We show that, perhaps paradoxically, the zero-error helper capacity can be calculated as a function of the description rate even for some channels for which the no-help zero-error capacity is unknown. This is not a contradiction because a zero-rate description is not tantamount to no description: it still allows for a binary description whose length is sublinear in the blocklength.

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

$$Y_k = x_k \oplus Z_k, \tag{1}$$

where $\{Z_k\} \sim$ IID Q_Z is the channel noise; x_k, Z_k, and Y_k all take values in the set $\mathcal{A} = \{0, 1, \ldots, |\mathcal{A}|-1\}$; and "$\oplus$" denotes mod-$|\mathcal{A}|$ addition. The channel law $Q_{Y|X}(\cdot|\cdot)$ is thus

$$Q_{Y|X}(y|x) = Q_Z(y \ominus x), \quad x, y \in \mathcal{A}, \tag{2}$$

where "$\ominus$" denotes mod-$|\mathcal{A}|$ subtraction. A key role is played by the cardinality $|\mathcal{S}|$ of the support set $\mathcal{S}$ of Q_Z,

$$\mathcal{S} = \{z \in \mathcal{A} \colon Q_Z(z) > 0\}. \tag{3}$$

Example 1. *With $|\mathcal{S}| = 2$, the MMANCs when $|\mathcal{A}|$ equals 3, 5, or 7 correspond respectively to the Triangle channel, Shannon's Pentagon channel [1], or the Heptagon channel (a.k.a. the $3/2$, $5/2$, or $7/2$ channels, respectively).*

In the presence of a noiseless feedback link from the receiver to the encoder, we calculate the zero-error helper capacity both for encoder and decoder assistance (Theorem 4). In its absence we show that, with zero-rate help (to the encoder or decoder), the zero-error capacity is positive if, and only if, the support $\mathcal{S}$ of the noise is a strict subset of $\mathcal{A}$ (Theorem 6). When the cardinality of $\mathcal{A}$ is prime (as in Example 1) we calculate the zero-error helper capacity in Theorem 5 using structured codes. Calculating the zero-error helper capacity without feedback when $|\mathcal{A}|$ is not prime is left as an open problem.

These results add to the body of literature on the benefits of helpers as measured in terms of the Shannon capacity[1] [3]–[5], error exponents [6], erasures-only capacity [5], listsize capacity [5], [7], and secrecy [8].

II. Preliminaries and Notations

For a general discrete memoryless channel (DMC) $Q_{Y|X}(\cdot|\cdot)$ with input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$, a blocklength-n code consists of a message set $\mathcal{M} = \{1, 2, \ldots, |\mathcal{M}|\}$ and an encoding function $f \colon \mathcal{M} \to \mathcal{X}^n$, $m \mapsto \mathbf{x}(m) = (x_1(m), \ldots, x_n(m))$. The code is also represented by the codebook $\mathcal{C} = \{\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(|\mathcal{M}|)\}$, which is a multiset (i.e., a set allowing repeated elements) of cardinality $|\mathcal{M}|$.

The *zero-error capacity* C_0 [1] is the supremum of rates R for which there exists a sequence of blocklength-n code with $\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{M}| = R$ and for which to every output sequence $\mathbf{y} \in \mathcal{Y}^n$ there corresponds at most one compatible message, i.e., a message $m \in \mathcal{M}$ satisfying

$$Q^n_{Y|X}(\mathbf{y}|\mathbf{x}(m)) > 0. \tag{4}$$

A necessary and sufficient condition for C_0 to be positive is that there exist $x, x' \in \mathcal{X}$ such that $Q_{Y|X}(y|x) \cdot Q_{Y|X}(y|x') = 0$ for all $y \in \mathcal{Y}$ [1]. This characterization can be used, for example, to conclude that C_0 is zero for the Triangle channel. Whenever C_0 is positive, we can transmit a bit by using the channel once (with the input x or x'). Consequently, C_0 cannot be positive yet strictly smaller than one.

Determining the zero-error capacity for general DMCs is an open combinatorial problem and is one of the holy grails of information theory. It is known for some specific channels including the Pentagon channel: Shannon showed that $\frac{1}{2} \log 5 \le C_0 \le \log \frac{5}{2}$ in his 1959 paper [1], and Lovász proved in 1979, using algebraic graph theory, that the lower bound is tight [9]. To date, however, the zero-error capacity of the $7/2$ channel is unknown.

[1]Throughout this paper, "Shannon capacity" and "Shannon feedback capacity" refer to the supremum of the achievable rates, in the sense that the probability of error tends to zero as the blocklength tends to infinity [2].

The problem is greatly simplified if a noiseless feedback link reveals to the encoder the previously received channel outputs. A blocklength-n encoder now consists of functions $f_i\colon \mathcal{M} \times \mathcal{Y}^{i-1} \to \mathcal{X}$, $(m, y^{i-1}) \mapsto x_i(m, y^{i-1})$ for $i \in [n] \triangleq \{1, 2, \ldots, n\}$, and the *zero-error feedback capacity* $C_{0\text{F}}$ is defined like C_0 except that $\mathbf{x}(m)$ in (4) is replaced by $\mathbf{x}(m, \mathbf{y}) = (x_1(m), x_2(m, y_1), \ldots, x_n(m, y^{n-1}))$. The capacity $C_{0\text{F}}$ for this setting was determined by Shannon:

Theorem 2 ([1])**.** *On a DMC, if $C_0 = 0$, then the zero-error feedback capacity $C_{0\text{F}}$ is also zero. Else, $C_{0\text{F}} = -\log \pi_0$, where*

$$\pi_0 = \min_{P \in \mathcal{P}(\mathcal{X})} \max_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}_y} P(x) \tag{5}$$

and $\mathcal{X}_y$ comprises the inputs that can induce the output letter y with positive probability.

Note that, $C_{0\text{F}} > 0$ iff $C_0 > 0$, so $C_{0\text{F}} > 0$ iff a bit can be transmitted error-free in one channel use. Hence, also $C_{0\text{F}}$ cannot be positive yet strictly smaller than one. Applying Theorem 2 to the MMANC yields the following corollary.

Corollary 3. *On the MMANC, if $C_0 = 0$, the zero error feedback capacity is also zero. Else,*

$$C_{0\text{F}} = \log |\mathcal{A}| - \log |\mathcal{S}|. \tag{6}$$

Proof. Omitted. □

Henceforth, we focus on MMANCs. Consider a helper in a blocklength-n coding scheme, represented by the helping function $h\colon \mathcal{A}^n \to \mathcal{T}$, that is incognizant of the transmitted message M, but that observes the noise sequence $\mathbf{Z}$ and describes it as $T = h(\mathbf{Z})$, with T taking values in a finite set $\mathcal{T}$. We distinguish between two kinds of assistance:

Decoder assistance corresponds to the scenario where the description T is revealed to the decoder, as in Fig. 1a. In the absence of feedback, with rate-R_{h} help, $C_{0,\text{dec}}(R_{\text{h}})$ is defined as the supremum of rates R for which there exists a sequence of coding schemes, with transmission rate—defined as $\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{M}|$—being at least R, with help rate—defined as $\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{T}|$—being no larger than R_{h}, and with zero probability of error, i.e., for any $\mathbf{y} \in \mathcal{A}^n$ and $t \in \mathcal{T}$, at most one message m is compatible with $(\mathbf{y}, t)$ in the sense that

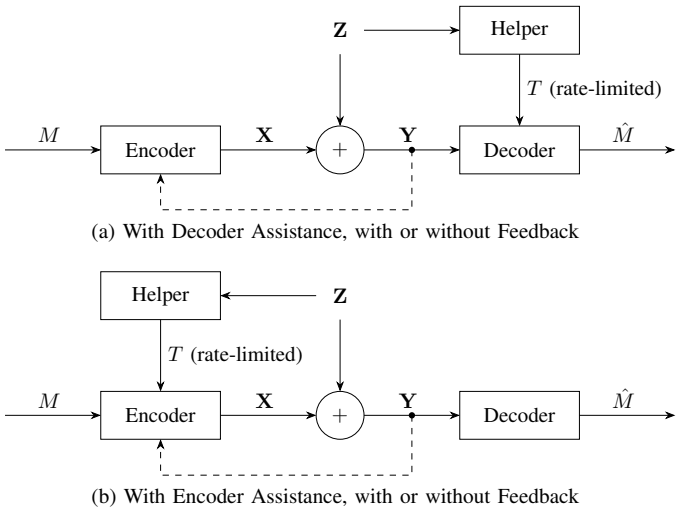
$$Q_{Y|X}^n(\mathbf{y}|\mathbf{x}(m)) > 0 \text{ and } h(\mathbf{y} \ominus \mathbf{x}(m)) = t. \tag{7}$$

With feedback, $C_{0\text{F,dec}}(R_{\text{h}})$ is defined by replacing $\mathbf{x}(m)$ with $\mathbf{x}(m, \mathbf{y})$ in (7).

Encoder assistance corresponds to the scenario where T is revealed noncausally to the encoder, as in Fig. 1b. In the absence of feedback, the encoding function is $f\colon \mathcal{M} \times \mathcal{T} \to \mathcal{A}^n$, $(m, t) \mapsto \mathbf{x}(m, t)$, and for given R_{h}, $C_{0,\text{enc}}(R_{\text{h}})$ is defined similarly so that to every $\mathbf{y} \in \mathcal{A}^n$ there corresponds at most one compatible message m in the sense that[2]

$$\exists t \in \mathcal{T} \text{ s.t. } Q_{Y|X}^n(\mathbf{y}|\mathbf{x}(m, t)) > 0 \text{ and } h(\mathbf{y} \ominus \mathbf{x}(m, t)) = t. \tag{8}$$

[2]This condition is equivalent to $Q_{\mathbf{Y}|M}(\mathbf{y}|m) > 0$, where $Q_{\mathbf{Y}|M}(\mathbf{y}|m) = \sum_{t\in\mathcal{T}} Q_T(t) Q_{\mathbf{Y}|\mathbf{X},T}(\mathbf{y}|\mathbf{x}(m, t), t)$.



(a) With Decoder Assistance, with or without Feedback

(b) With Encoder Assistance, with or without Feedback

Fig. 1. Modulo-Additive Noise Channels

With feedback, the encoder employs functions $f_i\colon \mathcal{M} \times \mathcal{T} \times \mathcal{A}^{i-1} \to \mathcal{A}$, $(m, t, y^{i-1}) \mapsto x_i(m, t, y^{i-1})$ for $i \in [n]$, and $C_{0\text{F,enc}}(R_{\text{h}})$ is defined by replacing $\mathbf{x}(m, t)$ by $\mathbf{x}(m, t, \mathbf{y}) = (x_1(m, t), x_2(m, t, y_1), \ldots, x_n(m, t, y^{n-1}))$ in (8).

Throughout this paper, logarithms are of base 2 unless stated otherwise. The positive integers are denoted $\mathbb{Z}^+$. For $\mathcal{B}, \mathcal{B}' \subseteq \mathcal{A}^n$, we define $\mathcal{B}^* = \mathcal{B} \setminus \{\mathbf{0}\}$; we denote the sumset and the difference set by

$$\mathcal{B} \oplus \mathcal{B}' = \{\mathbf{b} \oplus \mathbf{b}' \colon \mathbf{b} \in \mathcal{B},\, \mathbf{b}' \in \mathcal{B}'\} \tag{9}$$

$$\mathcal{B} \ominus \mathcal{B}' = \{\mathbf{b} \ominus \mathbf{b}' \colon \mathbf{b} \in \mathcal{B},\, \mathbf{b}' \in \mathcal{B}'\}; \tag{10}$$

and for $\mathbf{x} \in \mathcal{A}^n$, we write $\mathbf{x} \oplus \mathcal{B}$ and $\mathbf{x} \ominus \mathcal{B}$ for $\{\mathbf{x}\} \oplus \mathcal{B}$ and $\{\mathbf{x}\} \ominus \mathcal{B}$. We use $\{\xi\}^+$ to denote $\max\{0, \xi\}$.

III. Main Results

Theorem 4 (Assistance and Feedback)**.** *On the MMANC with feedback and rate-R_{h} decoder or encoder assistance,*

$$C_{0\text{F,dec}}(R_{\text{h}}) = C_{0\text{F,enc}}(R_{\text{h}}) = \log |\mathcal{A}| - \big\{ \log |\mathcal{S}| - R_{\text{h}} \big\}^+. \tag{11}$$

Proof. See Section IV. □

Theorem 5 (Assistance without Feedback)**.** *On the MMANC with rate-R_{h} decoder or encoder assistance, if $|\mathcal{A}|$ is prime, then*

$$C_{0,\text{dec}}(R_{\text{h}}) = C_{0,\text{enc}}(R_{\text{h}}) = \log |\mathcal{A}| - \big\{ \log |\mathcal{S}| - R_{\text{h}} \big\}^+. \tag{12}$$

Proof. See Section V-A. □

Theorem 6 (Positivity without Feeback)**.** *On the MMANC with zero-rate decoder or encoder assistance, the following three statements are equivalent:*

1) *$C_{0,\text{dec}}(0) = 0$;*
2) *$C_{0,\text{enc}}(0) = 0$;*
3) *$\mathcal{S} = \mathcal{A}$, i.e., the noise distribution Q_Z is of full support.*

Proof. If $\mathcal{S} = \mathcal{A}$ and the assistance is of zero rate, then—even with feedback—the zero-error capacities are zero (Theorem 4), let alone in its absence. It thus remains to establish that, when

$\mathcal{S}$ is a strict subset of $\mathcal{A}$, both $C_{0,\text{dec}}(0)$ and $C_{0,\text{enc}}(0)$ are positive. This follows from Lemma 12 in Section V-B ahead, i.e., from the lower bound in (43). □

The above theorems have some noteworthy implications:

Remark 7. *Assistance can increase the zero-error capacity by more than its rate. Even zero-rate assistance can increase the zero-error capacity. On the Pentagon channel, it raises the zero-error capacity to* $\log \frac{5}{2}$*, i.e., to* $C_{0\text{F}}$ *(Corollary 3). On the Triangle channel, it raises the zero-error capacity from zero to* $\log \frac{3}{2}$*, which is strictly positive and hence exceeds* $C_{0\text{F}}$*.*

Remark 8. *As on the Gel'fand-Pinsker channel with feedback [10], in all cases (with or without feedback, and with decoder or encoder assistance), transmitting one bit error-free may require more than one channel use. This is not the case in the absence of assistance.*

IV. Feedback Link Present

In this section, we study the zero-error feedback capacity with helper and establish Theorem 4; see Fig. 1a and 1b with the feedback link. To this end, we need the following lemma.

Lemma 9. *On the MMANC with feedback and rate-*R_h *decoder or encoder assistance, the Shannon capacities are given by*

$$C_{\text{F,dec}}(R_\text{h}) = C_{\text{F,enc}}(R_\text{h}) = \log|\mathcal{A}| - \big\{H(Q_Z) - R_\text{h}\big\}^+. \quad (13)$$

Proof. In light of [3, Theorem 12] and [4, Theorem 8], which establish that the RHS of (13) can be achieved without feedback, we only need to prove a converse. To that end, we prove the stronger claim that—even if the description T is presented to both encoder and decoder—the Shannon feedback capacity does not exceed the RHS of (13). We assume $R_\text{h} \le H(Q_Z)$, because otherwise the result is obvious.

Let M be a uniformly drawn message, then for any sequence of coding schemes of rate R with rate-R_h assistance and vanishing probabilities of error, we have

$$\begin{aligned}
\log|\mathcal{M}| &= H(M) && (14)\\
&= I(M;\mathbf{Y},T) + H(M|\mathbf{Y},T) && (15)\\
&= I(M;\mathbf{Y},T) + n\delta_n && (16)\\
&= I(M;\mathbf{Y}|T) + n\delta_n && (17)\\
&= H(\mathbf{Y}|T) - H(\mathbf{Y}|M,T) + n\delta_n && (18)\\
&\le H(\mathbf{Y}) - H(\mathbf{Y}|M,T) + n\delta_n && (19)\\
&\le H(\mathbf{Y}) - H(\mathbf{Z}|M,T) + n\delta_n && (20)\\
&= H(\mathbf{Y}) - H(\mathbf{Z}|T) + n\delta_n && (21)\\
&= H(\mathbf{Y}) - H(\mathbf{Z}) + I(\mathbf{Z};T) + n\delta_n && (22)\\
&\le H(\mathbf{Y}) - H(\mathbf{Z}) + \log|\mathcal{T}| + n\delta_n && (23)\\
&\le n\log|\mathcal{A}| - nH(Q_Z) + \log|\mathcal{T}| + n\delta_n, && (24)
\end{aligned}$$

where (16) holds for some $\{\delta_n\}$ tending to zero by Fano's inequality; (17) and (21) hold because T is a function of $\mathbf{Z}$, so $(\mathbf{Z},T)$ is independent of M; and (20) holds because in the presence of feedback and help, $\mathbf{Z}$ is a function of $(\mathbf{Y},M,T)$ namely $Z_i = Y_i \ominus f_i(M,T,Y^{i-1})$ for $i \in [n]$. Dividing the inequalities by n and letting n tend to infinity establish the converse. □

Proof of Theorem 4. We first establish the converse for decoder assistance. If $\tilde{Q}_{Y|X}$ is any auxiliary MMANC over $\mathcal{A}$ of noise distribution $\tilde{Q}_Z \in \mathcal{P}(\mathcal{A})$ that is absolutely continuous with respect to Q_Z (i.e., whose support is contained in $\mathcal{S}$, denoted by $\tilde{Q}_Z \ll Q_Z$), then its Shannon feedback capacity with decoder assistance $\tilde{C}_{\text{F,dec}}(R_\text{h})$ forms an upper bound on $C_{0\text{F,dec}}(R_\text{h})$, because any error-free coding scheme for the original channel is also error-free on the auxiliary channel. Indeed, for any $\mathbf{y} \in \mathcal{A}^n$ and $t \in \mathcal{T}$, the absolute continuity hypothesis implies that

$$\Big(\tilde{Q}^n_{Y|X}(\mathbf{y}|\mathbf{x}(m,\mathbf{y})) > 0\Big) \implies \Big(Q^n_{Y|X}(\mathbf{y}|\mathbf{x}(m,\mathbf{y})) > 0\Big) \quad (25)$$

so if a message m is compatible with $(\mathbf{y},t)$ on the auxiliary channel (in the sense that $\tilde{Q}^n_{Y|X}(\mathbf{y}|\mathbf{x}(m,\mathbf{y})) > 0$ and $h(\mathbf{y} \ominus \mathbf{x}(m,\mathbf{y})) = t$), then it is also compatible with $(\mathbf{y},t)$ on the original channel.

Therefore,

$$\begin{aligned}
C_{0\text{F,dec}}(R_\text{h}) &\le \min_{\tilde{Q}_Z\,:\,\tilde{Q}_Z \ll Q_Z} \tilde{C}_{\text{F,dec}}(R_\text{h}) && (26)\\
&= \min_{\tilde{Q}_Z\,:\,\tilde{Q}_Z \ll Q_Z} \Big\{\log|\mathcal{A}| - \big\{H(\tilde{Q}_Z) - R_\text{h}\big\}^+\Big\} && (27)\\
&= \log|\mathcal{A}| - \{\log|\mathcal{S}| - R_\text{h}\}^+, && (28)
\end{aligned}$$

where (27) follows from Lemma 9. Similar arguments apply also to encoder assistance.

We now turn to the direct part.

- Case 1: $R_\text{h} \ge \log|\mathcal{S}|$. In this case feedback is unnecessary. The codebook comprises all the distinct sequences in $\mathcal{A}^n$. Using $\lceil n\log|\mathcal{S}|\rceil$ bits, the helper can describe the noise sequence $\mathbf{Z}$ precisely. The decoder (resp. encoder) subtracts the noise from the received sequence (resp. from the codeword to be transmitted), so the codeword and the message can be received error-free. This establishes the achievability of $\log|\mathcal{A}|$ bits per channel use.
- Case 2: $R_\text{h} = 0$. A two-phase coding scheme is proposed. In Phase 1, we follow Shannon's construction in his proof of Theorem 2 [1], where the encoder repeatedly reduces the decoder's ambiguity. In the i-th channel use, thanks to the feedback, the encoder reconstructs the list of messages compatible with Y^{i-1} and evenly assigns them to different input symbols (in some way that is agreed upon with the decoder ahead of transmission). Only $|\mathcal{S}|$ out of $|\mathcal{A}|$ input symbols are compatible with Y_i, and the number of compatible messages is reduced by a factor of roughly $\frac{|\mathcal{S}|}{|\mathcal{A}|}$. More precisely, Shannon showed that if $|\mathcal{M}| = \big\lfloor\big(\frac{|\mathcal{S}|}{|\mathcal{A}|}\big)^{-n}\big\rfloor$, then after n channel uses, the number of compatible messages is at most $|\mathcal{A}|^2$. The final ambiguity is removed in Phase 2, where the helper comes into play. Since the list of compatible messages is of maximal length $|\mathcal{A}|^2$ and known to the encoder, it can inform the decoder which element of the list is the correct one in two additional channel uses. This information can be

conveyed error-free as long as the helper informs the decoder (resp. encoder) of the exact value of $Z_{n+1}^{n+2} \in \mathcal{S}^2$ and the decoder (resp. encoder) subtracts the noise after (resp. before) the transmission. The rate of help is therefore

$$\lim_{n\to\infty} \frac{1}{n+2} \log |\mathcal{S}|^2 = 0 \tag{29}$$

and the transmission rate

$$\lim_{n\to\infty} \frac{1}{n+2} \log |\mathcal{M}| = \lim_{n\to\infty} \frac{\log \left\lfloor \left(\frac{|\mathcal{S}|}{|\mathcal{A}|}\right)^{-n} \right\rfloor}{n+2} = \log \frac{|\mathcal{A}|}{|\mathcal{S}|}. \tag{30}$$

• Case 3: $0 < R_{\mathrm{h}} < \log |\mathcal{S}|$. We divide the transmission block into two parts of relative length $\frac{R_{\mathrm{h}}}{\log |\mathcal{S}|}$ and $1 - \frac{R_{\mathrm{h}}}{\log |\mathcal{S}|}$. We then apply the aforementioned coding schemes for helper rates of $\log |\mathcal{S}|$ and zero, respectively. The total rate achieved by this time-sharing scheme is

$$\begin{aligned} &\frac{R_{\mathrm{h}} \log |\mathcal{A}|}{\log |\mathcal{S}|} + \left(1 - \frac{R_{\mathrm{h}}}{\log |\mathcal{S}|}\right) \big(\log |\mathcal{A}| - \log |\mathcal{S}|\big) \\ &\quad = \log |\mathcal{A}| - \log |\mathcal{S}| + R_{\mathrm{h}}. \end{aligned} \tag{31}$$

□

V. Feedback Link Absent

In this section, we study the zero-error helper capacity in the absence of feedback, as in Fig. 1a and 1b without the feedback link.

A. Prime Cardinality

We begin with the case where $|\mathcal{A}|$ is a prime. Before proving Theorem 5 we remark that it, together with Merhav's upper bound on the Reliability Function with encoder assistance [6, Eq.(57)][3], characterizes the range of rates for which the Reliability Function is infinite:

Remark 10. *When $|\mathcal{A}|$ is prime, the Reliability Function of the MMANC with encoder assistance is infinite or finite depending on whether the rate is smaller or larger than $\log |\mathcal{A}| - \big\{ \log |\mathcal{S}| - R_{\mathrm{h}} \big\}^+$.*

Proof of Theorem 5. Since feedback cannot hurt, it follows from Theorem 4 that we only need to prove the direct part. This is trivial unless $|\mathcal{S}| < |\mathcal{A}|$, which we proceed to assume. We first focus on decoder assistance.

• Case 1: $R_{\mathrm{h}} \geq \log |\mathcal{S}|$. Follows from the proof for Theorem 4, where feedback is ignored.

• Case 2: $R_{\mathrm{h}} = 0$. We will construct a sequence of blocklength-n codebooks of rate $\big(\log \frac{|\mathcal{A}|}{|\mathcal{S}|} - \epsilon_n\big)$ that can be decoded error-free utilizing rate-ϵ_n' decoder assistance, for some $\{\epsilon_n\}$ and $\{\epsilon_n'\}$ tending to zero.

The codes we construct have two key properties. The first is that they are L-*list-decodable* where $\mathrm{L} \in \mathbb{Z}^+$ grows subexponentially with n. That is, every $\mathbf{y} \in \mathcal{A}^n$ is compatible with at most L messages. This guarantees that the decoder's ambiguity could be eliminated with a sublinear number of bits. Elias [11] established the existence such codebooks of rate $\log \frac{|\mathcal{A}|}{|\mathcal{S}|} - \Theta(\mathrm{L}^{-1})$. But this is not enough, because, in the absence of feedback, neither the transmitter nor the helper can determine the list facing the decoder. This is where the second property comes in: To overcome this issue and enable the helper to remove the ambiguity, we shall introduce a linear structure on the code, and this is where the assumption that $|\mathcal{A}|$ is a prime will be essential: it will allow us to view $\mathcal{A}$ as a field.

The existence of structured L-list-decodable codes can be established using a variation on a theme by Elias [11]. Specifically, we need the following lemma.

Lemma 11. *Consider a MMANC with $|\mathcal{A}| = p$, where p is prime. Given $\mathrm{L} \in \mathbb{Z}^+$, define*

$$R_{\mathrm{L}} = \max\left\{0,\, \log \frac{|\mathcal{A}|}{|\mathcal{S}|} - \frac{\log^2 |\mathcal{A}|}{\log(\mathrm{L}+1)}\right\}. \tag{32}$$

Then, for any $n \in \mathbb{Z}^+$, there exists a blocklength-n linear code over the field $\mathbb{F}_p$ of rate $\frac{\log |\mathcal{A}|}{n} \big\lfloor \frac{n R_{\mathrm{L}}}{\log |\mathcal{A}|} \big\rfloor$ that is L-list-decodable.

Proof. Omitted. □

We now use Lemma 11 to complete the proof of Theorem 5 for the case of $R_{\mathrm{h}} = 0$. Let $\{\mathrm{L}_n\}$ be a sequence of positive integers tending to infinity subexponentially, e.g., $\mathrm{L}_n = \Theta(n)$. The lemma implies that, for every blocklength n, there exists a linear code $\mathcal{C}_n$ of rate $\frac{\log |\mathcal{A}|}{n} \big\lfloor \frac{n R_{\mathrm{L}_n}}{\log |\mathcal{A}|} \big\rfloor$ that is L_n-list-decodable. The code $\mathcal{C}_n'$ we propose to use is the subset of $\mathcal{C}_n$ comprising all the distinct elements in $\mathcal{C}_n$. It satisfies: (i) $\mathcal{C}_n'$ is a subgroup of $\mathbb{Z}_p^n$, (ii) $\mathcal{C}_n'$ is L_n-list-decodable, and (iii)

$$|\mathcal{C}_n| \geq |\mathcal{C}_n'| \geq \frac{|\mathcal{C}_n|}{\mathrm{L}_n}. \tag{33}$$

This latter property and the fact that $\{\mathrm{L}_n\}$ is subexponential imply that $\{\mathcal{C}_n'\}$ has the desired rate:

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{C}_n'| &= \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{C}_n| && (34)\\ &= \lim_{n\to\infty} R_{\mathrm{L}_n} && (35)\\ &= \lim_{n\to\infty} \log \frac{|\mathcal{A}|}{|\mathcal{S}|} - \frac{\log^2 |\mathcal{A}|}{\log(\mathrm{L}_n+1)} && (36)\\ &= \log \frac{|\mathcal{A}|}{|\mathcal{S}|}, && (37) \end{aligned}$$

where (34) follows from (33) and the fact that $\{\mathrm{L}_n\}$ is subexponential; and (37) holds because $\{\mathrm{L}_n\}$ tends to infinity.

We next show that—although the helper is incognizant of the list—a $\lceil \log \mathrm{L}_n \rceil$-bit description of the noise sequence (which is of zero rate as L_n is subexponential in the blocklength n) suffices to guarantee zero-error transmission of the codebook $\mathcal{C}_n'$. To this end, we propose the following helper. To simplify its description, we drop the subscript n. For $\mathbf{z}, \mathbf{z}' \in \mathcal{S}^n$, let us write $\mathbf{z} \sim \mathbf{z}'$ if their componentwise difference is in $\mathcal{C}'$, i.e.,

$$\big(\mathbf{z} \sim \mathbf{z}'\big) \iff \big(\mathbf{z} \ominus \mathbf{z}' \in \mathcal{C}'\big), \quad \mathbf{z}, \mathbf{z}' \in \mathcal{S}^n. \tag{38}$$

[3] If $R > \log |\mathcal{A}| - \big\{ \log |\mathcal{S}| - R_{\mathrm{h}} \big\}^+$, then $\tilde{Q}_Z = \mathrm{Unif}(\mathcal{S})$ is feasible for the minimization in [6, Eq.(57)], hence its RHS is finite.

Since $\mathcal{C}'$ is a subgroup of $\mathbb{Z}_p^n$, this relation is an equivalence relation, and $\mathbf{z} \sim \mathbf{z}'$, i.e., $\mathbf{z}$ and $\mathbf{z}'$ are equivalent, if, and only if, $\mathbf{z}$ and $\mathbf{z}'$ belong to a same coset of $\mathcal{C}'$.

Our proposed helper assigns labels to noise sequences in $\mathcal{S}^n$ in such a way that *nonidentical equivalent noise sequences are assigned differing labels.* To see why such a helper leads to zero errors, note that if $\mathbf{x} \in \mathcal{C}'$ is transmitted and $\mathbf{x} \oplus \mathbf{z}$ is received (where $\mathbf{z} \in \mathcal{S}^n$), then the decoder can confuse $\mathbf{x}$ with some $\mathbf{x}'$ only if: $\mathbf{x}'$ is also a codeword; $\mathbf{x} \oplus \mathbf{z} = \mathbf{x}' \oplus \mathbf{z}'$ for some $\mathbf{z}' \in \mathcal{S}^n$; and $\mathbf{z}$ and $\mathbf{z}'$ have the same label. The former two conditions imply that $\mathbf{z} \sim \mathbf{z}'$, and hence that $\mathbf{z}$ and $\mathbf{z}'$ are identical or of differing labels. The third condition then implies that they are, in fact, identical, so $\mathbf{x}'$ equals $\mathbf{x}$.

It remains to verify that we can find a labeling rule as above with L different labels. This will follow once we show that, for every $\mathbf{z} \in \mathcal{S}^n$,

$$\big|[\mathbf{z}]\big| \le \mathrm{L}. \tag{39}$$

This inequality follows from the L-list-decodability property of $\mathcal{C}'$, i.e., that for every $\mathbf{y} \in \mathcal{A}^n$,

$$\mathrm{L} \ge \big|\big(\mathbf{y} \ominus \mathcal{C}'\big) \cap \mathcal{S}^n\big|. \tag{40}$$

Because $\mathcal{C}'$ is a subgroup of $\mathbb{Z}_p^n$, this is equivalent to

$$\mathrm{L} \ge \big|\big(\mathbf{y} \oplus \mathcal{C}'\big) \cap \mathcal{S}^n\big|, \tag{41}$$

so each coset of $\mathcal{C}'$ intersects $\mathcal{S}^n$ in at most L points, and (39) follows. This establishes the achievability.

- Case 3: $0 < R_{\mathrm{h}} < \log|\mathcal{S}|$. Follows by time sharing.

The case with encoder assistance is essentially identical. If $R_{\mathrm{h}} \ge \log|\mathcal{S}|$, the rate $\log|\mathcal{A}|$ is achievable as in the proof of Theorem 4. If $R_{\mathrm{h}} = 0$, the relation

$$C_{0,\mathrm{enc}}(0) \ge C_{0,\mathrm{dec}}(0) \tag{42}$$

holds because, in the presence of encoder assistance, any zero-rate help to the encoder can be conveyed to the decoder with negligible extra help and negligible loss in rate: the encoder simply appends a frame to convey the help, with the frame being of sublinear length (because the help to be conveyed is of zero rate); it requests that the helper provide it with a precise description of the noise affecting the frame (with the extra help being negligible because the frame is short); and it subtracts that noise from the transmission in that frame so as to render it noise free. For intermediate values of R_{h}, the achievability follows by time sharing. □

B. General Case

For the general case where $|\mathcal{A}|$ may not be a prime, we provide the following lower bound, which, together with Theorem 4, established Theorem 6.

Lemma 12 (Zero-Rate Helper and No Feedback)**.** *The zero-error capacity of the MMANC with zero-rate decoder or encoder assistance satisfies*

$$C_{0,\mathrm{enc}}(0) \ge C_{0,\mathrm{dec}}(0) \ge \frac{1}{2}\big(\log|\mathcal{A}| - \log|\mathcal{S}|\big). \tag{43}$$

Proof of Lemma 12. Omitted. □

REFERENCES

[1] C. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[2] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[3] 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.

[4] 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.

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

[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] 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

[8] S. Loyka and N. Merhav, "The secrecy capacity of the Gaussian wiretap channel with rate-limited help at the decoder," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 1040–1045.

[9] L. Lovász, "On the Shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, no. 1, pp. 1–7, 1979.

[10] A. Bracher and A. Lapidoth, "The zero-error feedback capacity of state-dependent channels," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3538–3578, 2018.

[11] P. Elias, "Zero error capacity under list decoding," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1070–1074, 1988.