On the Capacity of Scalar Gaussian Channels Subject to State Obfuscation

by

Omri Yaacov Lev

B.Sc., Technion—Israel Institute of Technology (2016)
M.Sc., Tel-Aviv University (2021)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

May 2024

Authored by: Omri Yaacov Lev
Department of Electrical Engineering and Computer Science
May 17, 2024

Certified by: Gregory W. Wornell
Sumitomo Professor of Engineering,
Thesis Supervisor

Accepted by: Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

On the Capacity of Scalar Gaussian Channels Subject to State Obfuscation

by

Omri Yaacov Lev

Submitted to the Department of Electrical Engineering and Computer Science
on May 17, 2024 in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

ABSTRACT

The problem of communication over multiple variants of the scalar Gaussian fading channel subject to a state-obfuscation constraint imposed in the form of near independence between the channel outputs and the channel coefficients has been studied. By defining the operational capacity as the maximal achievable rate under the state obfuscation constraint, an informational counterpart is been derived, which is then proved to coincide with the operational capacity. Conditions for this capacity to be non-zero and closed-form solutions for that capacity in the high signal-to-noise ratio (SNR) limit are derived.

Thesis supervisor: Gregory W. Wornell
Title: Sumitomo Professor of Engineering

Acknowledgments

First of all, I am deeply grateful to my advisor, Professor Gregory Wornell, for his invaluable guidance, support, and mentorship during the past two years. Throughout my research journey at MIT, Greg has been a constant source of insight and guidance, providing thoughtful suggestions and encouragement for me to explore the fundamentals of research problems. Greg has always agreed to meet with me and always brought a sense of humor and encouragement to our meetings.

I would also like to express my sincere gratitude to Prof. Ligong Wang and Matthew Ho, my collaborators, who have contributed to the success of this work. Your invaluable insights contributed significantly to the success of this thesis.

I also thank the current and former labmates in the Signals, Information and Algorithms (SIA) laboratory: Abhin Shah, Toros Arikan, Tejas Jayashankar, Gary Lee, Safa Medin, Mumin Jin, Maohao Shen, Dr. Jongha Ryu, and Dr. Amir Weiss. I am fortunate to have had the opportunity to collaborate with such a talented and supportive group of individuals. I would like to further express my sincere gratitude to Dr. Amir Weiss, whose guidance and friendship throughout my first semester at MIT alleviated the shock of arriving in a new country, and to Prof. Yuval Kochman and Prof. Meir Feder for multiple encouraging discussions on their occasional visits to our lab.

I wish to thank the faculty members at Tel-Aviv University: Prof. Ram Zamir and Prof. Uri Erez, who taught me the basic Information Theory classes and for whom I owe my admission into MIT's graduate program, and Prof. Anatoly Khina, my former supervisor, whose inspirational guidance was the number one reason for me to continue on my academic journey.

I would also like to express heartfelt gratitude to my family for their unwavering support and endless love.

Last but not least, I thank my life partner and my wife, Shiran, whose support and love were the most vital ingredients to the success of this thesis. Looking at the way we went together here, our relationship is my biggest achievement.

Contents

Chapter 1

Introduction

The inherent hardware imperfections of chipsets become apparent in the transmitted signal, which, combined with the physical location of the transmitter, give rise to a distinct radiometric fingerprint. This fingerprint can serve as a means of inferring the transmitter's location and enhancing security through additional authentication measures. Notably, recent studies propose practical fingerprinting solutions that can be readily implemented in commercial off-the-shelf devices [1], [2]. However, channel state information (CSI)-based localization and user identification have been demonstrated to be possible in multiple scenarios, which could seriously threaten people's privacy at home or workplace [3]. Moreover, since these parameters can be intercepted by gaining remote access to the hardware (e.g., through unsecured internet connections) or by employing low-cost sensing nodes, malicious applications can potentially infer users' identities and locations remotely, exploiting their sensitive information for nefarious purposes. Consequently, a growing number of applications aim to design improved physical-layer waveforms that make such unauthorized eavesdropping tasks more difficult [3]–[9].

This thesis investigates aspects of this issue from an information-theoretic perspective, determining when we can reliably communicate with a positive rate over a channel that is completely *obfuscated*. In this thesis, we seek to characterize the *obfuscated capacity* of multiple variants of the scalar Gaussian fading channel, i.e., the capacity subject to an additional obfuscation constraint in the form of near independence between the channel fading coefficients and the channel outputs. Our investigation builds upon the recent advancements in communication subject to state obfuscation made by Wang and Wornell [10], which focused on discrete memoryless state-dependent channels. In particular, our work aims to connect state obfuscation to physical channels by looking at the various variants of the Gaussian channel.

The rest of the thesis is organized as follows. In Chapter 2, we present the problem setup, and in Chapter 3, we present background material on the problems of communication subject to state masking, communication subject to state obfuscation, and non-coherent communication over Gaussian channels. We calculate the obfuscated capacity of the scalar Gaussian channel, with and without Channel State Information (CSI), for the case of memoryless, quasistatic, and correlated fading, with and without feedback, in Chapter 4. We calculate the obfuscated capacity of the intersymbol interference (ISI) channel in chapter 5. Chapter 6 discusses several directions for future research.

1.1 Notation:

We use bold upper- and lower-case letters for matrices and vectors, respectively. We denote random variables using san-serif fonts (x, y) and their realizations using regular italic fonts (x, y). We use $\mathbb{C}^{m\times n}$ and $\mathbb{C}^m$ to denote the sets of $m \times n$ complex matrices and $m \times 1$ complex vectors, respectively. The (i, j)-element of a matrix $\boldsymbol{A}$ is denoted by $\boldsymbol{A}[i, j]$. A block-diagonal matrix whose block-diagonal elements (which are themselves matrices) are $\{\boldsymbol{A}_i\}_{i=1}^k$ is denoted by $\operatorname{diag}(\boldsymbol{A}_1, \ldots, \boldsymbol{A}_k)$. The Euclidean norm is denoted by $\|\boldsymbol{a}\| \triangleq \sqrt{\sum_{i=1}^k |a_i|^2}$. The transpose of a matrix is denoted by $(\cdot)^T$ and the Hermitian transpose by $(\cdot)^\dagger$. For $j \geq i$, we denote $x_i^j \triangleq (x_i, \ldots, x_j)^T$; when $i = 1$, we simply write $x^j \triangleq x_1^j$. When i is not in numerical order but rather out of a set $\mathscr{A}$, we denote $\{x_i\}_{i\in\mathscr{A}}$. We usually denote sequences with infinite length by $\{\mathsf{x}_\ell\}$. The joint probability density function (PDF) of (x, y) is denoted by $P_{\mathsf{x},\mathsf{y}}(\cdot, \cdot)$. We denote the probability of an event A occurring to be $\mathbb{P}[A]$. The phase of a complex number x is denoted by $\angle x$. We denote $[n] \triangleq \{1, \ldots, n\}$. We use the notation $o(x)$ when $\lim_{x\to\infty} \frac{o(x)}{x} = 0$. We denote mutual information by $I(\cdot;\cdot)$ and differential entropy by $h(\cdot)$.

Chapter 2

Channel and System Model

This chapter introduces the channel models and the communication settings that will be analyzed throughout this thesis.

2.1 Channel Model

We consider two-channel models with additive Gaussian noise. The first is the scalar *fading* channel, described by

$$\mathsf{y}_n = \mathsf{h}_n \mathsf{x}_n + \mathsf{z}_n, \ n = 1, \ldots, N \tag{2.1}$$

where x_n and y_n are the transmitted and received signals at time n, respectively; the additive noises $\{\mathsf{z}_n\}$ are i.i.d. circularly symmetric complex Gaussian random variables with mean zero and variance $\frac{1}{\mathrm{SNR}}$; We assume $\mathsf{z}^N \perp\!\!\!\perp \mathsf{h}^N$, and since the transmitter does not know z^N then further $\mathsf{x}^N \perp\!\!\!\perp \mathsf{z}^N$. We further assume that the fading coefficients have a bounded variance, namely $\mathbb{E}\left[|\mathsf{h}_n|^2\right] < \infty, \forall n \in [N]$. We will consider multiple different scenarios regarding the distribution of the multiplicative gains $\{\mathsf{h}_n\}$: We will refer to the case where the sequence $\{\mathsf{h}_n\}$ is i.i.d. as the *memoryless fading* case; for the case where $\mathsf{h}_n = \mathsf{h}, \forall n \in [N]$ as the *quasi-static fading* case; and for the general case where the channel coefficients are neither constant nor i.i.d. as *correlated fading*. For any N, let $\mathsf{t}_N \sim \mathrm{Unif}\left(\{1, \ldots, N\}\right)$ and define the random variables $\tilde{\mathsf{h}}_{\mathsf{t}_N}$. Then, we assume this sequence converges (as $N \to \infty$) in distribution to a random variable h. For the memoryless fading case, the distribution of h is the same as the marginal distribution of every h_n.[1]

The second model we consider is the *discrete-time ISI* channel (see [11], [12] and references therein)

$$\mathsf{y}_n = \sum_{\ell=1}^{L} \mathsf{h}_\ell \mathsf{x}_{n-\ell+1} + \mathsf{z}_n, \ n = 1, \ldots, N \tag{2.2}$$

where x_n, y_n, and z_n are the same as in the first model; and where $\{\mathsf{h}_\ell\} : \mathsf{h}_\ell \in \mathbb{C}, \forall \ell$ is the (truncated) channel impulse response. For any N, we assume that L is constant s.t.

[1] We note that by the bounded second-moment assumption on the fading coefficients, we further have $\mathbb{E}\left[|\mathsf{h}|^2\right] < \infty$.

$L < N$. However, we allow L to grow with N as long as its asymptotic behavior is $L \in o(N)$. Moreover, we assume that $\sum_{\ell=1}^{\infty} \mathbb{E}\left[|\mathsf{h}_\ell|^2\right] < \infty$. We can then define the frequency response of the length-L channel by

$$\mathsf{H}_L(f) \triangleq \sum_{\ell=1}^{L} \mathsf{h}_\ell e^{-j2\pi(\ell-1)f}, \quad 0 \le f < 1$$

and we further define $\mathsf{H}(f) = \lim_{L\to\infty} \mathsf{H}_L(f)$. We assume that the function $|\mathsf{H}(f)|$ is continuous over $[0,1)$ w.p. 1.

2.2 Communication Setting

We now define the communication setting.

Encoder. observes a message $\mathsf{M} \in \left[2^{RN}\right]$ and generates a codeword via a sequence of random mappings from M to $\mathsf{x}_n \in \mathbb{C}$, $n = 1, \ldots, N$. We denote $\mathsf{x}^N \triangleq (\mathsf{x}_1, \ldots, \mathsf{x}_N)^T$. The codeword x^N is subject to an average input power constraint

$$\frac{1}{N}\sum_{n=1}^{N} \mathbb{E}\left[|\mathsf{x}_n|^2\right] \le 1$$

where the expectation is taken over a uniformly drawn message and the random encoding mappings. We will further analyze the case where we have Channel State Information (CSI) at the encoder, namely, the case where the symbol x_n is generated by a random mapping from the message M and the realization of channel coefficients. We will refer to the case of *causal* CSI as the case where $\mathsf{x}_n = f_n\left(\mathsf{M}, \mathsf{h}^{n-1}\right)$ and to the *noncausal* CSI case as the case where $\mathsf{x}_n = f_n\left(\mathsf{M}, \mathsf{h}^N\right)$.

Decoder. receives the channel outputs y^N and tries to decode the message M. We denote the decoded message by $\hat{\mathsf{M}}$.

Obfuscation Constraint. The channel outputs are subject to an obfuscation constraint of the form of near independence between the sequence y^N and the channel fading coefficients. For the memoryless and correlated fading channels, the constraint is

$$\lim_{N\to\infty} \frac{1}{N} I\left(\mathsf{y}^N; \mathsf{h}^N\right) = 0 \tag{2.3}$$

where for the quasi-static case, the constraint is

$$\lim_{N\to\infty} I\left(\mathsf{y}^N; \mathsf{h}\right) = 0 \tag{2.4}$$

For the ISI channel, the constraint is

$$\lim_{N\to\infty} I\left(\mathsf{y}_L^N; \mathsf{h}^L\right) = 0. \tag{2.5}$$

A rate R is said to be achievable if there exists a sequence of length-N codes such that the obfuscation constraint—(2.3) for the memoryless and correlated fading channels, (2.4) for the quasi-static fading channel and (2.5) for the ISI channel—is satisfied and the probability of decoding error $P\left(\hat{\mathsf{M}} \neq \mathsf{M}\right)$ approaches zero as $N \to \infty$. The *obfuscated capacity* is defined as the supremum of all achievable rates and is denoted by $C_{\text{ob}}(\text{SNR})$.

Remark 1. The channel (2.2) is an approximation for the sampled output of a continuous time convolution channel, with an impulse response that is truncated to length L. However, as $N \to \infty$, this approximation becomes accurate as long as $\lim_{t\to\infty} h(t) = 0$.

Chapter 3

Background

This chapter surveys the background material used to solve our problem. We introduce the communication problem subject to state masking, initially studied by Shamai and Merhav [13], and its original motivation for the *dirty paper* channel. Then, the state obfuscation problem, interpreted as an extreme case of state masking, is introduced, and its original discrete-state results derived by Wang and Wornell [10] are surveyed. We then continue to present results from the theory of non-coherent communication, which will be widely used throughout this thesis to calculate the Gaussian channel's obfuscated capacity. In particular, we will review classical results about the phase noise channel [14], [15] with Gaussian noise, showing the capacity expressions and their solutions for many scenarios of interest.

3.1 Communication Subject to State Masking

The problem of information transfer via state-dependent channels has been studied extensively in Information Theory (see [16]–[20]). One interesting model is the one where the channel states are available at the encoder, causally or noncausally. This framework has been fully characterized for i.i.d. states [17], [18]. These models have gained much interest in the communication society, driven by the enormous amount of applications associated with the celebrated *dirty-paper* framework [19], [21]–[25] (see also App. B), correspond to the Gaussian version of the Gelfand-Pinsker setting with states that impact the channel additively, namely, $\mathsf{y} = \mathsf{x} + \mathsf{s} + \mathsf{z}$, for some interfering state sequence s where x is subject to an input power constraint in the form of $\mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1$. While the source and channel states are usually assumed independent in the theoretical models, this is not always the case. In some applications, the channel–state process is not inherently channel–related (like in fading) but may rather be an information-bearing signal on its own. The MIMO broadcast channel serves as a typical example, where a state sequence for one user is just the information–carrying sequence for another, and all produced at the same encoder who addresses both users simultaneously [26]. This has driven the motivation that, in addition to maximizing communication rates, one might be interested in the information the receiver can gain about the unknown state sequence and design codes that try to simultaneously maximize the communication rate and *mask* information about the state sequence. The problem of state masking was studied initially by Merhav and Shamai [13], for a communication setting

defined via N instances of a memoryless state-dependent channel defined via the probability kernel $P_{\mathsf{y}|\mathsf{x},\mathsf{s}}$ and where the state sequence is assumed to be i.i.d. and known (causally and noncausally) to the encoder, with an additional masking constraint of leakage of less than E bits from the state sequence to the channel output, namely $\lim_{N\to\infty} \frac{1}{N} I\left(\mathsf{y}^N;\mathsf{s}^N\right) \leq E$. In that case, the optimal trade-off between R and E was proved to be characterized by the solution to the next problem (see [13, Thm. 2, Sec. V])

$$R \leq \sup \ \{I\left(\mathsf{u};\mathsf{y}\right) - I\left(\mathsf{u};\mathsf{s}\right)\}$$

where the supremum is over distributions of the form

$$P_{\mathsf{s},\mathsf{u},\mathsf{x},\mathsf{y}}\left(s,u,x,y\right) = P_{\mathsf{s}}(s)P_{\mathsf{u}}(u)P_{\mathsf{x}|\mathsf{u},\mathsf{s}}\left(x|u,s\right)W(y|x,s)$$

subject to

$$I\left(\mathsf{s};\mathsf{u},\mathsf{y}\right) \leq E, \quad \mathbb{E}\left[\phi(\mathsf{x})\right] \leq \Gamma$$

where $\phi(\mathsf{x})$ is an input constraint, imposed in the form of $\frac{1}{N}\sum_{n=1}^{N}\phi(\mathsf{x}_n) \leq \Gamma$. Following this single-letter characterization, closed-form solutions for the optimal (R,E) trade-off were derived for the Gaussian case (i.e. the case where s and z are Gaussian variables). The problem of communication subject to state masking has been further extended to multiple other communication settings, including state-dependent quantum channels [27], [28], integrated communication and sensing scenarios [29], secure source coding [30] and binary energy harvesting channels [31], and have been extended further beyond the communication realm, to characterize learning problems under fairness and privacy constraints [32], [33].

3.2 Communication Subject to State Obfuscation

The problem of communication subject to state obfuscation can be thought of as the extreme case of state masking, where we require the masking level E to be strictly zero, requiring a strict privacy criterion of leakage of (asymptotically) zero bits of information about the channel state to the receiver. A motivation for such a model is a scenario where the transmitter wishes to conceal its physical location, with the assumption that its location may affect the channel's statistics to the receiver; hence, it can be modeled as a channel state. The problem of communication subject to state obfuscation has been studied recently by Wang and Wornell [10] for the case where we communicate over a discrete memoryless channel (DMC) that is affected by a random state $s \in \mathcal{S}$, distributed according to some $P_{\mathsf{s}}(s)$ where both the input alphabet and the output alphabet of the DMC $\mathcal{X}$ and $\mathcal{Y}$ and the state alphabet $\mathcal{S}$ are assumed to be finite. A set of probabilities thus characterizes the DMC transitions $\{W(y|x,s)\}_{x\in\mathcal{X},y\in\mathcal{Y},s\in\mathcal{S}}$ and the communication scenario is defined similarly to that of Sec. 2.2, without the power constraint. In contrast to the state-masking problem, and driven by the potential application of concealing physical locations, the problem of state obfuscation is studied for multiple different options of the temporal structure of the state sequence s^N, including the case where the state remains constant during the entire transmission, instead of the i.i.d. assumption that has been made in [13]. To that end, we review the different results derived in [10]. We start by examining the case with CSI.

3.2.1 State Obfuscation With CSI

In that case, the communication setting is defined similarly to that of Sec. 2.2 with CSI. The obfuscation constraint is given by (2.3) for the case where the channel states are i.i.d. and by (2.4) for the case where the channel state is assumed to be constant throughout the entire duration of communication. We will refer to the later case as the *(quasistatic)* case.

Lemma 1 (Obfuscated Capacity With CSI [10])**.** *When the encoder has either causal or noncausal CSI, the obfuscated capacity for the case where the states are i.i.d. and for the case where the state is quasistatic is given by*

$$C_{\text{ob}} = \sup \; I\left(\mathsf{u};\mathsf{y}\right)$$

where the supremum is over distributions of the form

$$P_{\mathsf{s},\mathsf{u},\mathsf{x},\mathsf{y}}\left(s,u,x,y\right) = P_{\mathsf{s}}(s)P_{\mathsf{u}}(u)P_{\mathsf{x}|\mathsf{u},\mathsf{s}}\left(x|u,s\right)W(y|x,s)$$

subject to

$$I\left(\mathsf{s};\mathsf{u},\mathsf{y}\right) = 0$$

We note that the i.i.d. case with CSI can be easily proved by adapting the single letter solution of the state masking problem and imposing the hard constraint of $E = 0$, yielding independence between u and s.

3.2.2 State Obfuscation Without CSI

The case where the transmitter has no CSI has been treated differently between the cases where we allow the encoder to be deterministic, namely, a deterministic function from the message M to the input codeword x^N and the stochastic case described in Sec. 2.2. Moreover, different results were derived for the i.i.d. case and the quasistatic case. To that end, we give the single-letter expressions derived for the i.i.d. case with a stochastic encoder and those derived for the quasistatic case with a deterministic encoder.

Lemma 2 (Obfuscated Capacity Without CSI [10])**.** *Without CSI, the obfuscated capacity for the case where the state is i.i.d. and we use a stochastic encoder is given by an argument similar to Lem. 1, with $P_{\mathsf{x}|\mathsf{u},\mathsf{s}}(x|u,s)$ replaced by $P_{\mathsf{x}|\mathsf{u}}(x|u)$. When we use a deterministic encoder, the obfuscated capacity with i.i.d. states and with quasistatic states is given by*

$$C_{\text{ob}} = \sup \; I\left(\mathsf{x};\mathsf{y}\right)$$

where the supremum is over distributions of the form

$$P_{\mathsf{s},\mathsf{x},\mathsf{y}}\left(s,x,y\right) = P_{\mathsf{s}}(s)P_{\mathsf{x}}\left(x\right)W(y|x,s)$$

subject to

$$I\left(\mathsf{s};\mathsf{x},\mathsf{y}\right) = 0$$

Interestingly, in that case, a single-letter expression for the obfuscated capacity for the quasistatic case with a stochastic encoder remains an open problem. However, by the problem definition, it is known to be upper bounded by the expression derived for the quasistatic case with CSI and lower bounded by the expression derived for the deterministic encoder case. Later in the thesis, we will show that, for the Gaussian case, a single-letter upper bound, which is tight asymptotically, can be derived.

3.3 Non-Coherent Communication over Gaussian Phase-Noise Channels

In this section, we review some classical results on the non-coherent capacity of phase-noise channels with additive Gaussian noise. The term *phase-noise channel* refers to channels as the channel (2.1), and where the multiplicative gains $\{\mathsf{h}_n\}$ are assumed to have a constant magnitude. The results we present here follow from the classical results of Lapidoth [14] and Nuriyev *et al.*[34]. Throughout this section, we denote by $o(1)$ terms that tend to zero as the SNR $\to \infty$.

3.3.1 Memoryless and Correlated Phase-Noise Channel

The memoryless phase-noise channel is the channel (2.1) with i.i.d. sequence $\{\mathsf{h}_n\}$ and where $|\mathsf{h}_n|$ is constant with probability (w.p.) 1. Its *non-coherent capacity*, denoted by $C_{\text{nc}}(\text{SNR})$, is the maximal achievable rate R in the same setting as we described in Sec. 2.2, but *without* the obfuscation constraint. (The terminology "non-coherent" refers to the fact that the decoder is oblivious to the values of the sequence h^N.) In a similar sense, the correlated phase-noise channel is defined in a similar way, where now we assume that the channel coefficients have constant magnitude and that $h\left(\{\angle \mathsf{h}_i\}\right) > -\infty$. The asymptotic (as SNR $\to \infty$) non-coherent capacity for those channels was derived by Lapidoth [14].

Lemma 3 ([14])**.** *Consider the channel (2.1) and assume that $|\mathsf{h}_n| = \tilde{h}, \forall n \in [N]$ w.p. 1 for some positive constant $\tilde{h}$, and that $h\left(\{\angle \mathsf{h}_n\}\right) > -\infty$, where $\angle \mathsf{h}_i$ denotes the phase of h_i. Then,*

$$C_{\text{nc}}(\text{SNR}) = \frac{1}{2}\log\left(\text{SNR}\right) \cdot \left(1 + o(1)\right)$$

We note that the memoryless fading case is a private case of Lem. 3. In that case, the requirements translates to $|\mathsf{h}| = \tilde{h}$ w.p. 1 and $h(\angle \mathsf{h}) > -\infty$. Moreover, for the memoryless case, it can be proved that the capacity is the solution for the next optimization problem

$$C_{\text{nc}}(\text{SNR}) = \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right] \le 1} I\left(\mathsf{x};\mathsf{y}\right).$$

3.3.2 Quasistatic Phase-Noise Channel

The quasi-static phase-noise channel is the channel (2.1) where $\mathsf{h}_n = \mathsf{h}, \forall n \in [N]$ and when $|\mathsf{h}|$ is constant w.p. 1. Its non-coherent capacity is defined similarly to that in the memoryless

case and was analyzed in [34]. We now state the results from [34] in a more convenient way, which will prove useful in this thesis

Lemma 4 ([34])**.** *Consider the channel* (2.1) *where* $\mathsf{h}_n = \mathsf{h}, \forall n \in [N]$ *and assume that* $|\mathsf{h}| = \tilde{h}$ *w.p.* 1 *for some positive constant* $\tilde{h}$*. Then,*

$$C_{\text{nc}}(\text{SNR}) = \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1} I(\mathsf{x};\mathsf{y}). \tag{3.1}$$

If further $h(\angle \mathsf{h}) > -\infty$ *then,*

$$C_{\text{nc}}(\text{SNR}) = \log(\text{SNR}) \cdot (1 + o(1)) \tag{3.2}$$

Proof. The single letter form (3.1) and the lower bound of (3.2) were derived in [34]. The upper bound of (3.1) follows trivially by the classical results on the capacity of the (coherent) Gaussian channel. □

3.4 Independence in Addition

Throughout the analysis, we will use the next lemma to characterize independence between random variables connected via a channel with additive independent noise.

Lemma 5. *Let* $\mathsf{h}, \mathsf{x}, \mathsf{z} \in \mathbb{C}$ *be random variables s.t.* $\mathsf{z} \perp\!\!\!\perp (\mathsf{hx}, \mathsf{h})$ *and let* $\mathsf{y} = \mathsf{hx} + \mathsf{z}$*. Then* $\mathsf{y} \perp\!\!\!\perp \mathsf{h}$ *if and only if* $\mathsf{hx} \perp\!\!\!\perp \mathsf{h}$*.*

Proof. Using characteristic function to test independence between random variables [35, Ch. 7], $\mathsf{y} \perp\!\!\!\perp \mathsf{h}$ implies

$$\phi_{\mathsf{y},\mathsf{h}}(v_1, v_2) = \phi_{\mathsf{y}}(v_1)\phi_{\mathsf{h}}(v_2) \tag{3.3}$$

where $\phi_{\mathsf{w}}(v) \triangleq \mathbb{E}\left[e^{j\mathsf{w}v}\right]$ is the characteristic function of w. Using the independence between h, x and z we get

$$\begin{aligned} \phi_{\mathsf{y},\mathsf{h}}(v_1, v_2) &= \phi_{\mathsf{z}}(v_1)\phi_{\mathsf{hx},\mathsf{h}}(v_1, v_2), \\ \phi_{\mathsf{y}}(v) &= \phi_{\mathsf{hx}}(v)\phi_{\mathsf{z}}(v) \end{aligned} \tag{3.4}$$

where $\phi_{\mathsf{w}_1,\mathsf{w}_2}(v_1, v_2) \triangleq \mathbb{E}\left[e^{j(\mathsf{w}_1 v_1 + \mathsf{w}_2 v_2)}\right]$. Combining (3.3) and (3.4) yields the necessary and sufficient condition:

$$\phi_{\mathsf{hx},\mathsf{h}}(v_1, v_2) = \phi_{\mathsf{hx}}(v_1)\phi_{\mathsf{h}}(v_2)$$

which implies that $\mathsf{hx} \perp\!\!\!\perp \mathsf{h}$. □

The next lemma, which is a consequence of Lem. 5 will allow us to characterize the capacity of Gaussian channels subject to state obfuscation constraint

Lemma 6. *Let* $\mathsf{h}, \mathsf{x}, \mathsf{z} \in \mathbb{C}$ *be random variables s.t.* $\mathsf{z} \perp\!\!\!\perp (\mathsf{hx}, \mathsf{h})$ *and* $\mathsf{x} \perp\!\!\!\perp \mathsf{h}$ *and let* $\mathsf{y} = \mathsf{hx} + \mathsf{z}$*. Then* $\mathsf{y} \perp\!\!\!\perp \mathsf{h}$ *implies that* $|\mathsf{h}|$ *is constant w.p.* 1 *or* $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$*.*

Proof. By Lem. 5, $\mathsf{y} \perp\!\!\!\perp \mathsf{h}$ if and only if $\mathsf{hx} \perp\!\!\!\perp \mathsf{h}$. In particular, this requires that $\mathbb{E}\left[|\mathsf{hx}|^2 \,\middle|\, \mathsf{h} = \tilde{h}\right] = \left|\tilde{h}\right|^2 \mathbb{E}\left[|\mathsf{x}|^2\right]$ must not depend on h, which can be true only if either $|\mathsf{h}|$ is constant or $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$. □

Chapter 4

The Obfuscated Capacity of the Scalar Gaussian Channel

In this chapter, we will derive the obfuscated capacity for multiple variants of the scalar Gaussian channel defined in (2.1). Starting with the cases of memoryless and quasistatic fading, we will adapt the results of Lem. 1 and Lem. 2 for our Gaussian setting for the case where the transmitter has CSI and for the case where the transmitter does not have CSI. For the case without CSI, we will prove a single-letter upper bound on the obfuscated capacity with quasistatic fading, which will be asymptotically tight, as opposed to the discrete case, which currently lacks a single-letter expression. We will further analyze the case where we have feedback, and we will prove that, asymptotically, feedback can not increase the obfuscated capacity of the Gaussian channel (both in the memoryless and the quasistatic case). We will then further analyze the case of correlated fading. We will give a conjecture and an informal reasoning for the conditions for which the obfuscated capacity is non-negative, and under some additional technical assumptions we will derive a single-letter upper bound on that capacity, for which we will then solve to derive the capacity in an asymptotic closed form.

4.1 Memoryless and Quasistatic Fading

4.1.1 Obfuscated Capacity With CSI

We will start with the case where we have CSI, for which the results of [10] can be directly extended to the scalar Gaussian channel.

Lemma 7. *The obfuscated capacity of the memoryless fading and the quasi-static fading channels with causal or non-causal CSI, denoted by* $C_{\text{ob}}^{\text{CSI}}(\text{SNR})$*, is greater than zero only if* $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$.

Proof. Repeating the proof of [10, Thm. 1, Thm. 5] and adding the power constraint, we get that the obfuscated capacity for the cases of memoryless and quasi-static fading, with causal or non-causal CSI, is given by

$$C_{\text{ob}}^{\text{CSI}} = \sup \; I\left(\mathsf{u};\mathsf{y}\right)$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}}(h,u,x,y) = P_{\mathsf{h}}(h)P_{\mathsf{u}}(u)P_{\mathsf{x}|\mathsf{u},\mathsf{h}}(x|u,h)\,P_{\mathsf{y}|\mathsf{x},\mathsf{h}}(y|x,h)$$

subject to

$$I(\mathsf{h};\mathsf{u},\mathsf{y}) = 0, \quad \mathbb{E}\left[|\mathsf{x}|^2\right] \le 1.$$

We note that $I(\mathsf{h};\mathsf{u},\mathsf{y}) = 0$ implies $I(\mathsf{h};\mathsf{y}) = 0$, which further by Lem. 5 implies $\mathsf{hx} \perp\!\!\!\perp \mathsf{h}$. Thus, we have that $c \triangleq \mathbb{E}\left[|\mathsf{hx}|^2 \middle| \mathsf{h} = \tilde{h}\right] = \left|\tilde{h}\right|^2 \mathbb{E}\left[|\mathsf{x}|^2 \middle| \mathsf{h} = \tilde{h}\right]$ is independent of $\tilde{h}$. In particular, we note that

$$\mathbb{E}\left[\frac{c}{|\mathsf{h}|^2}\right] = c \cdot \mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] = \mathbb{E}\left[\mathbb{E}\left[|\mathsf{x}|^2 \middle| \mathsf{h} = \tilde{h}\right]\right] = \mathbb{E}\left[|\mathsf{x}|^2\right] \le 1$$

Thus, whenever $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] = \infty$, we must have $c = 0$ which implies that $\mathsf{hx} = 0$ almost always, leading to $\mathsf{y} \perp\!\!\!\perp \mathsf{x}$ and thus a capacity of 0. □

We now use Lem. 7 to characterize the capacity of the memoryless fading and the quasi-static fading channels with CSI.

Theorem 1. *Let y^N be the output of the channel (2.1) with causal or non-causal CSI, and assume that $\mathbb{E}\left[\frac{1}{|\mathsf{h}|^2}\right] < \infty$. Then*

$$C_{\text{ob}}^{\text{CSI}} = \log(\text{SNR}) \cdot (1 + o(1))$$

Proof. We first prove the converse. Using Cauchy-Schwarz inequality, we note that $S \triangleq \mathbb{E}\left[|\mathsf{hx}|^2\right] < \infty$ [1]. Then, since (u,h)—hx—y forms a Markov chain, we can upper bound the capacity by that of a coherent Gaussian channel

$$\mathsf{y}^\star = \mathsf{x}^\star + \mathsf{z}$$

where $\mathsf{x}^\star \triangleq \mathsf{hx}$, with the power constraint $\mathbb{E}\left[|\mathsf{x}^\star|^2\right] \le S$. This further tells us that

$$C_{\text{ob}}^{\text{CSI}} \le \log(S \cdot \text{SNR}) \cdot (1 + o(1)) = \log(\text{SNR}) \cdot (1 + o(1))$$

where the $\log(S)$ term was included inside the $o(1)$ terms.

Now, we prove the lower bound by providing a construction that achieves the same asymptotic behavior. Let $\bar{\mathsf{h}}_n \triangleq \frac{1}{\mathsf{h}_n\sqrt{\mathbb{E}\left[1/|\mathsf{h}|^2\right]}}$ and let the input sequence x^N be given by $\mathsf{x}_n = \bar{\mathsf{h}}_n\tilde{\mathsf{x}}_n$ where $\tilde{\mathsf{x}}_n$ are i.i.d symmetric complex Gaussian random variables with zero mean and unit variance. We first note that $\mathbb{E}\left[|\mathsf{x}_n|^2\right] = \mathbb{E}\left[\left|\bar{\mathsf{h}}_n\right|^2\right]\mathbb{E}\left[|\tilde{\mathsf{x}}_n|^2\right] = 1$, and thus it satisfies the power constraint. Furthermore, since $\mathsf{y}_n = \frac{1}{\sqrt{\mathbb{E}\left[1/|\mathsf{h}|^2\right]}}\tilde{\mathsf{x}}_n + \mathsf{z}_n$, we conclude that $\mathsf{y}_n \perp\!\!\!\perp \mathsf{h}^N$ and thus we further have $\mathsf{y}^N \perp\!\!\!\perp \mathsf{h}^N$ and the obfuscation constraint is satisfied. Using the

[1] Recall that we assumed that the channel has bounded second moment

classical arguments about the Gaussian channel [36, Ch. 3], we note that the maximum rate for which we can reliably transmit information with this scheme is given by the capacity of the Gaussian channel, which asymptotically is given by $\log(\mathrm{SNR})(1+o(1))$. Lastly, since the proof is the same for the causal and the non-causal cases, we conclude that the same capacity is attained in both scenarios. □

Remark 2. We note that the capacity is attained by a coding scheme that uses a *deterministic* encoder, similar to the constructions for the discrete case that was presented in [10].

4.1.2 Memoryless Fading Without CSI

We will now proceed to analyze the case where we do not have CSI, and the fading process is assumed to be i.i.d.. In that case, we will first adopt the results from the discrete-state case to prove a single-letter converse, from which we will derive the conditions for a non-zero obfuscated capacity. We will then calculate the obfuscated capacity in a closed form

Lemma 8. *The obfuscated capacity of the memoryless fading channel is upper-bounded as*

$$C_{\mathrm{ob}}(\mathrm{SNR}) \leq \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right]\leq 1} I\left(\mathsf{x};\mathsf{y}\right). \tag{4.1}$$

Furthermore, $C_{\mathrm{ob}}(\mathrm{SNR}) > 0$ *only if* $|\mathsf{h}|$ *is constant w.p.* 1.

Proof. Repeating the proof of [10, Thm. 3] and adding the power constraint we get that

$$C_{\mathrm{ob}} = \sup\ I\left(\mathsf{u};\mathsf{y}\right)$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}}\left(h,u,x,y\right) = P_{\mathsf{h}}(h)P_{\mathsf{u}}(u)P_{\mathsf{x}|\mathsf{u}}\left(x|u\right)P_{\mathsf{y}|\mathsf{x},\mathsf{h}}(y|x,h)$$

subject to

$$I\left(\mathsf{h};\mathsf{u},\mathsf{y}\right) = 0, \quad \mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1.$$

For an upper bound on C_{ob}, we first relax the condition $I\left(\mathsf{h};\mathsf{u},\mathsf{y}\right) = 0$ to $I\left(\mathsf{h};\mathsf{y}\right) = 0$. By Lem. 6 this requires that $|\mathsf{h}|$ is constant or $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$. Since $\mathbb{E}\left[|\mathsf{x}|^2\right] = 0$ clearly does not allow communication, we conclude that C_{ob} is nonzero only if $|\mathsf{h}|$ is constant w.p. 1. Further note that, since u—x—y forms a Markov chain, we have $I\left(\mathsf{u};\mathsf{y}\right) \leq I\left(\mathsf{x};\mathsf{y}\right)$. This completes the proof. □

We now use Lem. 8 to analyze the obfuscated capacity in the regime where $\mathrm{SNR} \to \infty$.

Theorem 2. *Let* y^N *be the output of the channel* (2.1) *with* $|\mathsf{h}| = \tilde{h} > 0$ *w.p.* 1. *Then*

$$C_{\mathrm{ob}} \geq \frac{1}{2}\log\left(\mathrm{SNR}\right)\cdot\left(1+o(1)\right).$$

If furthermore $h\left(\angle\mathsf{h}\right) > -\infty$, *then*

$$C_{\mathrm{ob}} = \frac{1}{2}\log\left(\mathrm{SNR}\right)\cdot\left(1+o(1)\right). \tag{4.2}$$

Proof. To prove the converse, we note that whenever $|\mathsf{h}|$ is constant, the right-hand side of (4.10) is the non-coherent capacity of the memoryless scalar phase-noise Gaussian channel, which by Lem. 3 is given by $\frac{1}{2}\log(\mathrm{SNR})\cdot(1+o(1))$ when $h(\angle\mathsf{h})>-\infty$.

We prove the lower bound by presenting a coding scheme. For the channel (2.1), let the input sequence x^N be given by $\mathsf{x}_n = e^{j\varphi_n}\tilde{\mathsf{x}}_n$, where $\{\varphi_n\}$ are i.i.d. and $\mathrm{Unif}([0,2\pi))$, and $\tilde{\mathsf{x}}_n = \sqrt{2\mathsf{S}_n}$ where $\{\mathsf{S}_n\}$ are i.i.d. with PDF $P_{\mathsf{S}}(S) = \frac{\sqrt{S}e^{-S}}{\int_0^\infty \sqrt{t}e^{-t}dt}$. Since $\mathbb{E}[2\mathsf{S}_n]=1$ [14], this input sequence satisfies the power constraint. Furthermore,

$$\mathsf{y}_n = \mathsf{h}_n e^{j\varphi_n}\tilde{\mathsf{x}}_n + \mathsf{z}_n \triangleq \tilde{\mathsf{h}}_n\tilde{\mathsf{x}}_n + \mathsf{z}_n$$

where, by [37, Ch. 4], $\{\angle\tilde{\mathsf{h}}_n\}$ is i.i.d. $\mathrm{Unif}([0,2\pi))$ and $\angle\tilde{\mathsf{h}}_n \perp\!\!\!\perp \angle\mathsf{h}_n$. Since $\left|\tilde{\mathsf{h}}_n\right| = \tilde{h}$ w.p. 1, this further implies that $\tilde{\mathsf{h}}_n \perp\!\!\!\perp \mathsf{h}_n$ and furthermore $\tilde{\mathsf{h}}_n\tilde{\mathsf{x}}_n \perp\!\!\!\perp \mathsf{h}_n$. Thus, by Lem. 5 we have $\mathsf{y}_n \perp\!\!\!\perp \mathsf{h}_n$, $\forall n\in[N]$. Since $\{\mathsf{h}_n,\mathsf{y}_n\}$ is i.i.d. in n, we have $I\left(\mathsf{y}^N;\mathsf{h}^N\right)=0$ so the obfuscation constraint is satisfied. Moreover, by considering the channel with input $\tilde{\mathsf{x}}^N$ and output y^N, we obtain a classic phase-noise channel, and by standard achievability arguments for memoryless channels, we can reliably communicate at rate $I(\tilde{\mathsf{x}};\mathsf{y})$ where $\tilde{\mathsf{x}}$ and y are random variables whose distributions are the same as those of $\tilde{\mathsf{x}}_n$ and y_n for every n. By [14, Sec. IV], as $\mathrm{SNR}\to\infty$, our choice for $\tilde{\mathsf{x}}_n$ yields $I(\tilde{\mathsf{x}};\mathsf{y}) = \frac{1}{2}\log(\mathrm{SNR})(1+o(1))$. This proves the lower bound. □

Remark 3 (Multiplexing Gain). When $h(\angle\mathsf{h})=-\infty$, (4.2) may not hold. To see this, consider the case where $\mathsf{h}\in\{\pm1\}$. Obfuscation can be achieved by multiplying the input symbols by a sequence a_n that is i.i.d. uniformly over $\{\pm1\}$. Roughly speaking, we can transmit two real symbols per channel use (the real and the imaginary parts of the input symbol), resulting in a multiplexing gain of 2 as opposed to 1 in (4.2).

.

4.1.3 Quasistatic Fading Without CSI

We now continue to calculate the obfuscated capacity of the Gaussian channel (2.1) with quasi-static fading, namely, the case where $\mathsf{h}_1=\ldots=\mathsf{h}_N=\mathsf{h}$. The proof follows the same lines for memoryless fading, where we first show that the $|\mathsf{h}|$ must be constant for a non-zero capacity. Then, we will use the capacity results of the block-noncoherent channel to derive the capacity.

Theorem 3. *The obfuscated capacity of the Gaussian channel with quasi-static fading is greater than zero only if $|\mathsf{h}|$ is constant w.p. 1 and is given by*

$$C_{\mathrm{ob}} = \log(\mathrm{SNR})\cdot(1+o(1)).$$

Proof. The obfuscation constraint tells us that, for any N, $I(\mathsf{y}_i;\mathsf{h})\le\epsilon_N, \forall i\in[N]$. By using Fano's inequality we get that $R-\tilde{\epsilon}_N \le \frac{1}{N}\sum_{n=1}^N I(\mathsf{u}_i;\mathsf{y}_i)$ where $\mathsf{u}_i\triangleq(\mathsf{M},\mathsf{y}^{i-1})$. Thus, using the same arguments as of [10, Thm. 6] we get the next single-letter upper bound on the capacity

$$C_{\mathrm{ob}} \le \sup\ I(\mathsf{u};\mathsf{y})$$

where the supremum is over distributions of the form

$$P_{\mathsf{h},\mathsf{u},\mathsf{x},\mathsf{y}}(h,u,x,y) = P_{\mathsf{h}}(h)P_{\mathsf{u}}(u)P_{\mathsf{x}|\mathsf{u},\mathsf{h}}(x|u,h)\,P_{\mathsf{y}|\mathsf{x},\mathsf{h}}(y|x,h)$$

subject to

$$I(\mathsf{h};\mathsf{y}) = 0, \quad \mathbb{E}\left[|\mathsf{x}|^2\right] \leq 1.$$

Thus, by the same reasonings as the previous proof, we conclude that $|\mathsf{h}|$ must be constant w.p. 1. To find the exact expression for the upper bound, we note that the obfuscated capacity in the quasi-static case and with constant $|\mathsf{h}| = \tilde{h}$ is upper bounded by the (coherent) capacity of a Gaussian channel whose SNR is $\left|\tilde{h}\right|^2 \cdot \mathrm{SNR}$. Then, the upper bound follows by the capacity of the classical Gaussian channel [36, Ch. 3]. We prove the lower bound by presenting a coding scheme. Let the input sequence x^N be given by $\mathsf{x}_n = e^{j\varphi}\tilde{\mathsf{x}}_n$, where $\varphi \sim \mathrm{Unif}([0,2\pi))$, and $\tilde{\mathsf{x}}_n = \mathsf{S}_n$ where $\{\mathsf{S}_n\}$ are i.i.d. complex Gaussian variables with zero mean and unit variance. This input sequence satisfies the power constraint, and similarly to the proof of Th. 2, it also satisfies the obfuscation constraint. Moreover, by considering the channel with input $\tilde{\mathsf{x}}^N$ and output y^N, we obtain a block non-coherent channel, which by using the sequence $\tilde{\mathsf{x}}^N$ and as $N \to \infty$ we can communicate reliably at rate $\log(\mathrm{SNR})(1+o(1))$ [34, Sec. IV.C]. This proves the lower bound. □

Remark 4. We note that in contrast to the discrete state case of [10], utilizing the Gaussianity of the underlying channel, we are able to derive the obfuscated capacity in (asymptotically) closed form for the "constant state" case. Moreover, following [34], that capacity can be approached by a coding scheme employing a differential phase encoding, where we further multiply the phases by a constant initial random phase factor.

Remark 5 (Deterministic Encoder). The analysis of Th. 2 and Th. 3 considered the stochastic encoder case, whereas the analysis in [10] separates between the case where one uses a stochastic encoder and the case where one uses a deterministic encoder. However, we note that the obfuscation constraint of the deterministic encoder case, given by (see [10]) $I(\mathsf{h};\mathsf{x},\mathsf{y}) = 0$ can not be satisfied in a Gaussian channel with deterministic encoder. To see this, note that $I(\mathsf{h};\mathsf{x},\mathsf{y}) = 0$ implies $I(\mathsf{h};\mathsf{y}|\mathsf{x}) = 0$, which is impossible to hold under the additive channel model unless $\mathsf{x} = 0$. As pointed out earlier, this is not true for the case where we have CSI at the encoder, for which the capacity is achieved by a coding scheme employing a *deterministic* encoder.

4.1.4 Obfuscated Capacity With Feedback

We now continue to analyze the obfuscated capacity where we have feedback.

Memoryless Fading With Feedback

We now show that feedback does not increase the obfuscated capacity of the memoryless fading channel.

Theorem 4. *Feedback does not increase the obfuscated capacity of the memoryless fading channel*

Proof. We note that when we add feedback, the next Markov relationship holds

$$\begin{gathered}\left(\mathsf{y}^{i-1},\mathsf{M}\right)\text{—}\mathsf{x}_i\text{—}\mathsf{y}_i,\ \forall i\in 1,\ldots,N,\\ \mathsf{M}\text{—}\mathsf{y}^N\text{—}\hat{\mathsf{M}}\end{gathered}\tag{4.3}$$

Thus, by defining the auxiliary variable $\mathsf{u}_i \triangleq (\mathsf{M},\mathsf{y}^{i-1})$ the same analysis of [10, Thm. 3] and Lem. 8 still holds and we get the same capacity expressions. The lower bound is thus by using the same coding schemes from Th. 2 and Th. 3, respectively. □

Remark 6. We note that this analysis does not use the fact that the underlying channel is Gaussian and holds for any memoryless channel. Thus, feedback does not increase the obfuscated capacity of memoryless channels.

Quasistatic Fading With Feedback

The next scenario we analyze is the case of quasistatic fading with feedback. The underlying Gaussian channel structure allows us to evaluate the capacity in an asymptotically closed form.

Theorem 5. *The obfuscated capacity of the Gaussian channel with quasistatic fading is greater than zero only if* $|\mathsf{h}|$ *is constant w.p.* 1 *and is given by*

$$C_{\text{ob}} = \log\left(\text{SNR}\right)\cdot\left(1+o(1)\right).$$

Proof. Similarly to Th. 4, the same Markov relations (4.3) holds in the quasistatic case. Thus, by defining the auxiliary variable $\mathsf{u}_i \triangleq (\mathsf{M},\mathsf{y}^{i-1})$ the same converse of Th. 3 still holds, and thus we conclude that $|\mathsf{h}|$ must be constant w.p. 1 to get a non-zero capacity. Then, the upper bound follows since feedback does not increase the capacity of the memoryless Gaussian channel (without obfuscation constraint), for which its asymptotic capacity is given by $\log(\text{SNR})\cdot(1+o(1))$ and which serves as an upper bound on the obfuscated capacity. The lower bound follows by the same coding scheme presented in Th. 3 □

Remark 7. We note that the analysis of the memoryless case does not use the fact that the underlying channel is Gaussian and holds for any memoryless channel. Thus, feedback does not increase the obfuscated capacity of memoryless channels. However, for the quasistatic case, the converse bound of Th. 3 holds only as an upper bound, which becomes tight asymptotically in the Gaussian case. A single-letter capacity result for the quasistatic case is yet to be developed.

4.2 Correlated Fading

We now proceed to the more involved case, where the fading process is not assumed to be i.i.d. nor constant but instead can have any temporal structure. As opposed to the previous chapters, the analysis in this section is more preliminary and still lacks the full derivation of the conditions for which the obfuscated capacity is non-zero and its closed-form solution in the most general case. However, we conjecture that under mild technical assumptions, the

obfuscated capacity is non-zero only if $|\mathsf{h}|$ is constant w.p. 1 and that we can achieve at most one degree of freedom for communication in this setting. We only consider cases where we do not have access to CSI.

4.2.1 Obfuscated Capacity With Correlated Fading

The correlated fading case is defined similarly to the previous cases based on the scalar fading channel (2.1) with the constraint (2.3). Unless otherwise specified, we assume that for any channel coefficient h_i, we have the property that, given h^{i-1}, h_i has the same support as h_1 w.p. 1. Concretely, we define the support of $\mathbb{C}^n$-valued random variable a as

$$\text{Supp}\left\{\mathsf{a}\right\} \triangleq \{x \in \mathbb{C}^n : P(\mathsf{a} \in B_r(x)) > 0,\ \forall r > 0\}$$

where $B_r(x)$ is the ball with radius r centered at x where we are using the Euclidean distance metric, and we similarly define the conditional support $\text{Supp}\left\{\mathsf{a}|\mathsf{b}\right\}$ where we now instead of $P(\mathsf{a} \in B_r(x))$ use the conditional probability $P\left(\mathsf{a} \in B_r(x)|\mathsf{b}\right)$. In other words, by denoting $\mathscr{H} \triangleq \text{supp}(\mathsf{h}_1)$, we are assuming that for any $i \in [N]$,

$$\text{Supp}\left\{\mathsf{h}_i|\mathsf{h}^{i-1}\right\} = \mathscr{H} \quad \text{w.p. } 1 \tag{4.4}$$

Beyond (4.4), we do not restrict the inter-dependence of the sequence of fading coefficients $\{\mathsf{h}_i\}$.

For this section, we denote by $W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ a Gaussian distribution with variance $\frac{1}{\text{SNR}}$ and mean hx that is evaluated on the point y. We start with our first conjecture, claiming that the obfuscated capacity is greater than zero only if $|\mathsf{h}|$ (as defined in Sec. 2.1) is constant w.p. 1.

Conjecture 1. *The obfuscated capacity of the Gaussian channel with correlated fading is greater than zero only if* $|\mathsf{h}|$ *is constant w.p.* 1.

We now justify this conjecture by providing informal proof. We then point out the missing point to make it fully proof.

Informal Reasoning 1. *We note that the absence of CSI and the obfuscation constraint*

tells us that for every N,

$$\begin{aligned}
N\hat{\epsilon}_N &\geq I\left(\mathsf{h}^N;\mathsf{M},\mathsf{y}^N\right)\\
&=\sum_{i=1}^{N} I\left(\mathsf{h}_i;\mathsf{M},\mathsf{y}^N\middle|\mathsf{h}^{i-1}\right)\\
&\geq\sum_{i=1}^{N} I\left(\mathsf{h}_i;\mathsf{M},\mathsf{y}^i\middle|\mathsf{h}^{i-1}\right)\\
&=\sum_{i=1}^{N}\left(I\left(\mathsf{h}_i;\mathsf{y}_i\middle|\mathsf{M},\mathsf{y}^{i-1},\mathsf{h}^{i-1}\right)+I\left(\mathsf{h}_i;\mathsf{M},\mathsf{y}^{i-1}\middle|\mathsf{h}^{i-1}\right)\right) &(4.5)\\
&\geq\sum_{i=1}^{N} I\left(\mathsf{h}_i;\mathsf{y}_i\middle|\mathsf{M},\mathsf{y}^{i-1},\mathsf{h}^{i-1}\right) &(4.6)\\
&=NI\left(\mathsf{h}_\mathsf{t};\mathsf{y}_\mathsf{t}|\mathsf{u}_\mathsf{t},\mathsf{t}\right) &(4.7)\\
&\triangleq NI\left(\mathsf{h};\mathsf{y}|\mathsf{u}\right) &(4.8)
\end{aligned}$$

where ϵ_N goes to 0 as $N\to\infty$, (4.5) is by the chain rule, (4.6) is since the MI is non-negative, and (4.7) is by defining $\mathsf{u}_i\triangleq(\mathsf{M},\mathsf{y}^{i-1},\mathsf{h}^{i-1})$ and defining the variable $\mathsf{t}\sim\mathrm{Unif}\left(\{1,\ldots,N\}\right)$ and (4.8) is by defining the variables $\mathsf{y}\triangleq\mathsf{y}_\mathsf{t}$, $\mathsf{u}\triangleq(\mathsf{u}_\mathsf{t},\mathsf{t})$ and $\mathsf{h}\triangleq\mathsf{h}_\mathsf{t}$ and using the chain rule [2]*. To upper bound the capacity, we use Fano's inequality to get*

$$\begin{aligned}
R-\epsilon_N &\leq \frac{1}{N}I\left(\mathsf{M};\mathsf{y}^N\right)\\
&=\frac{1}{N}\sum_{i=1}^{N} I\left(\mathsf{M};\mathsf{y}_i\middle|\mathsf{y}^{i-1}\right)\\
&\leq\frac{1}{N}\sum_{i=1}^{N} I\left(\mathsf{M},\mathsf{h}^i;\mathsf{y}_i\middle|\mathsf{y}^{i-1}\right)\\
&=\frac{1}{N}\sum_{i=1}^{N} I\left(\mathsf{h}^i;\mathsf{y}_i\middle|\mathsf{y}^{i-1}\right)+I\left(\mathsf{M};\mathsf{y}_i\middle|\mathsf{y}^{i-1},\mathsf{h}^i\right)\\
&\leq\frac{1}{N}I\left(\mathsf{h}^N;\mathsf{y}^N\right)+\frac{1}{N}\sum_{i=1}^{N} I\left(\mathsf{u}_i;\mathsf{y}_i|\mathsf{h}_i\right)\\
&=\frac{1}{N}I\left(\mathsf{h}^N;\mathsf{y}^N\right)+I\left(\mathsf{u}_\mathsf{t};\mathsf{y}_\mathsf{t}|\mathsf{h}_\mathsf{t},\mathsf{t}\right)\\
&\leq\tilde{\epsilon}_N+I\left(\mathsf{u};\mathsf{y}|\mathsf{h}\right)
\end{aligned}$$

where all the steps are by the chain rule and by the obfuscation constraint. Taking $N\to\infty$ and using the continuity of mutual information (see, for example, [10, Thm. 2]) and

[2] By the chain rule, $I\left(\mathsf{x};\mathsf{y}|\mathsf{w},\mathsf{z}\right)=I\left(\mathsf{x},\mathsf{w};\mathsf{y}|\mathsf{z}\right)-I\left(\mathsf{w};\mathsf{y}|\mathsf{z}\right)$. Thus, the chain rule further implies the inequality $I\left(\mathsf{x};\mathsf{y}|\mathsf{w},\mathsf{z}\right)\leq I\left(\mathsf{x},\mathsf{w};\mathsf{y}|\mathsf{z}\right)$

incorporating the power constraint, we note that this implies the next converse

$$C_{ob}\left(\mathrm{SNR}\right) \leq \sup_{P_{\mathsf{u}|\mathsf{h}}P_{\mathsf{x}|\mathsf{u}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right]\leq 1} I\left(\mathsf{u};\mathsf{y}|\mathsf{h}\right)$$

where the joint distribution is out of the form $P_{\mathsf{h}}P_{\mathsf{u}|\mathsf{h}}P_{\mathsf{x}|\mathsf{u}}W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ *subject to*

$$I\left(\mathsf{h};\mathsf{y}|\mathsf{u}\right)=0 \tag{4.9}$$

where u *is defined over some support* $\mathscr{U}$ *(which we further optimize over) and where we note that by (4.4) we have*

$$Supp\left\{\mathsf{h}|\mathsf{u}\right\}=\mathscr{H}\ \ w.p.\ 1$$

and where we used $W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ *since given* h_{t} *and* x_{t}, y_{t} *is distributed according to* $W_{\mathsf{y}|\mathsf{x},\mathsf{h}}(\cdot|\cdot,\cdot)$. *By the obfuscation constraint, we note that* $(\mathsf{y}|\mathsf{u}=u)\perp\!\!\!\perp(\mathsf{h}|\mathsf{u}=u)$ *w.p. 1. Since the channel* $W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ *is defined by a Gaussian channel law and since* x *is generated from* u *and since the support of* $\mathsf{h}|\mathsf{u}=u$ *is* $\mathscr{H}$ *w.p. 1, we have that for any* $u\in\mathscr{U}$ *such that* $(\mathsf{y}|\mathsf{u}=u)\perp\!\!\!\perp(\mathsf{h}|\mathsf{u}=u)$ *we must also have that* $(\mathsf{h}\mathsf{x}|\mathsf{u}=u)\perp\!\!\!\perp(\mathsf{h}|\mathsf{u}=u)$ *by applying Lem. 5, and then applying Lem. 13 we obtain that* $(|\mathsf{h}|\,|\mathsf{u}=u)$ *is constant w.p. 1. Then because* $\mathrm{Supp}\left\{\mathsf{h}|\mathsf{u}=u\right\}=\mathscr{H}$ *w.p.* 1, *we can conclude that w.p.* 1 *we have that both* $(|\mathsf{h}|\,|\mathsf{u}=u)$ *is constant and* $\mathrm{Supp}\left\{\mathsf{h}|\mathsf{u}=u\right\}=\mathscr{H}$, *implying that* $\mathscr{H}$ *is a subset of a circle and that* $|\mathsf{h}|$ *is constant w.p.* 1.

The open points are that, under this formulation, we do not have cardinality nor dimensionality bound on $\mathscr{U}$. Moreover, the major open point is in the requirement for $\mathbb{E}\left[\left|\mathsf{h}\cdot\mathsf{x}(\mathsf{u})\right|^2\middle|\mathsf{h},\mathsf{u}\right]$ being constant w.p. 1, where this requirement is vague when the alphabet of u is not specified. However, since this type of auxiliaries is common in many classical information theory problems (see, for example, [13, Thm. 2]), we believe that this conjecture is true.

We now proceed by assuming that the previous conjecture is true, namely, that $|\mathsf{h}|$ is constant w.p. 1, and prove a single-letter formula for the obfuscated capacity. We refer to the distribution of the h as the distribution of the angle of h, namely, $P_{\mathsf{h}}(h)$ refers to the PMF of the angle of h in the case of discrete phases and to the PDF of the angle in the continuous case.

Lemma 9. *Assuming that Conj. 1 is true, the obfuscated capacity of the Gaussian channel with correlated fading is greater than zero only if* $|\mathsf{h}|$ *is constant w.p.* 1 *and is upper-bounded as*

$$C_{\mathrm{ob}}(\mathrm{SNR}) \leq \sup_{P_{\mathsf{x}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right]\leq 1} I\left(\mathsf{x};\mathsf{y}\right). \tag{4.10}$$

where y *is defined via the channel* $\mathsf{y}=\mathsf{h}\mathsf{x}+\mathsf{z}$ *with* $\mathsf{z}\sim\mathcal{N}\left(0,\frac{1}{\mathrm{SNR}}\right)$.

Proof. Following the informal reasoning of Conj. 1, we have the next converse on the obfuscated capacity

$$C_{\mathrm{ob}}\left(\mathrm{SNR}\right) \leq \sup_{P_{\mathsf{u}|\mathsf{h}}P_{\mathsf{x}|\mathsf{u}}:\ \mathbb{E}\left[|\mathsf{x}|^2\right]\leq 1} I\left(\mathsf{u};\mathsf{y}|\mathsf{h}\right)$$

where the joint distribution is out of the form $P_{\mathsf{h}}P_{\mathsf{u}|\mathsf{h}}P_{\mathsf{x}|\mathsf{u}}W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ subject to

$$I\left(\mathsf{h};\mathsf{y}|\mathsf{u}\right)=0 \tag{4.11}$$

and where u is defined over some support $\mathscr{U}$, and where furthermore we know that this term is greater than zero only if $|\mathsf{h}|$ is constant w.p. 1. We will now simplify this bound. We first write (4.11) explicitly, namely,

$$\begin{aligned}I\left(\mathsf{h};\mathsf{y}|\mathsf{u}\right)&=\mathbb{E}_{\mathsf{u}}\left[\mathbb{E}_{\mathsf{y},\mathsf{h}|\mathsf{u}}\left[\log\left(\frac{dP_{\mathsf{y},\mathsf{h}|\mathsf{u}}}{d(P_{\mathsf{y}|\mathsf{u}}P_{\mathsf{h}|\mathsf{u}})}\right)\right]\right]\\&=\mathbb{E}_{\mathsf{u}}\left[D\left(P_{\mathsf{y}|\mathsf{h},\mathsf{u}}P_{\mathsf{h}|\mathsf{u}}\middle\|P_{\mathsf{y}|\mathsf{u}}P_{\mathsf{h}|\mathsf{u}}\right)\right]\end{aligned}$$

where $\frac{dP}{dQ}$ denotes the Radon-Nikodym derivative for the ratio of distributions, and the last equality is by the definition of the KL-divergence and by the definition of the conditional distribution, where the support condition tells us that the joint distributions are defined over $\mathbb{C}\times\mathscr{H}$. Since the KL-divergence is non-negative, (4.9) implies that

$$P_{\mathsf{y}|\mathsf{h},\mathsf{u}}(y|h,u)=P_{\mathsf{y}|\mathsf{u}}(y|u) \tag{4.13}$$

for almost all $y\in\mathbb{C},h\in\mathscr{H},u\in\mathscr{U}$ where "almost all" is taken with respect to the distributions of $\mathsf{y},\mathsf{u},\mathsf{h}$ respectively.

We now note that

$$\begin{aligned}I\left(\mathsf{u};\mathsf{y}|\mathsf{h}\right)&=\mathbb{E}_{\mathsf{h}}\left[\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[D\left(P_{\mathsf{y}|\mathsf{h},\mathsf{u}}\middle\|P_{\mathsf{y}|\mathsf{h}}\right)\right]\right]\\&=\mathbb{E}_{\mathsf{h}}\left[\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[D\left(P_{\mathsf{y}|\mathsf{u}}\middle\|P_{\mathsf{y}|\mathsf{h}}\right)\right]\right]\end{aligned} \tag{4.14}$$

where the second equality is by (4.13). Furthermore, using the obfuscation constraint, we get that

$$P_{\mathsf{y}|\mathsf{h}}=\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[P_{\mathsf{y}|\mathsf{h},\mathsf{u}}\right]=\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[P_{\mathsf{y}|\mathsf{u}}\right]$$

and by substituting it further into (4.14) we get

$$\begin{aligned}I\left(\mathsf{u};\mathsf{y}|\mathsf{h}\right)&=\mathbb{E}_{\mathsf{h}}\left[\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[D\left(P_{\mathsf{y}|\mathsf{u}}\middle\|\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[P_{\mathsf{y}|\mathsf{u}}\right]\right)\right]\right]\\&\leq\mathbb{E}_{\mathsf{h}}\left[\sup_{P_{\mathsf{u}|\mathsf{h}}}\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[D\left(P_{\mathsf{y}|\mathsf{u}}\middle\|\mathbb{E}_{\mathsf{u}|\mathsf{h}}\left[P_{\mathsf{y}|\mathsf{u}}\right]\right)\right]\right]\\&\leq\mathbb{E}_{\mathsf{h}}\left[\sup_{P_{\mathsf{u}}}\mathbb{E}_{\mathsf{u}}\left[D\left(P_{\mathsf{y}|\mathsf{u}}\middle\|\mathbb{E}_{\mathsf{u}}\left[P_{\mathsf{y}|\mathsf{u}}\right]\right)\right]\right] &(4.15a)\\&=\sup_{P_{\mathsf{u}}}\mathbb{E}_{\mathsf{u}}\left[D\left(P_{\mathsf{y}|\mathsf{u}}\middle\|\mathbb{E}_{\mathsf{u}}\left[P_{\mathsf{y}|\mathsf{u}}\right]\right)\right] &(4.15b)\\&=\sup_{P_{\mathsf{u}}}I\left(\mathsf{u};\mathsf{y}\right)\end{aligned}$$

where (4.15a) is since $P_{\mathsf{u}|\mathsf{h}}$ is defined over $\mathscr{U}$, and thus we can upper bound by maximizing the MI over input distributions defined on the alphabet $\mathscr{U}$, and (4.15b) is since the inner maximization is independent of h.

We conclude that we can further simplify the converse toward the next form

$$C_{\text{ob}}\left(\text{SNR}\right) \leq \sup_{P_{\mathsf{u}}P_{\mathsf{x}|\mathsf{u}}\colon\ \mathbb{E}\left[|\mathsf{x}|^2\right]\leq 1} I\left(\mathsf{u};\mathsf{y}\right)$$

where the joint distribution is out of the form $P_{\mathsf{h}}P_{\mathsf{u}}P_{\mathsf{x}|\mathsf{u}}W_{\mathsf{y}|\mathsf{x},\mathsf{h}}$ where u is defined over an alphabet $\mathscr{U}$ and where $\mathscr{H}$ is a subset of a circle. Since u—x—y forms a Markov chain, we have $I\left(\mathsf{u};\mathsf{y}\right) \leq I\left(\mathsf{x};\mathsf{y}\right)$ and this concludes the proof. □

Remark 8. To demonstrate why (4.4) is necessary, we now give an example that violates (4.4) and for which $|\mathsf{h}|$ does not have to be constant for a non-zero obfuscated capacity. Let the channel coefficients defined by $\mathsf{h}_{2n} = 1, \mathsf{h}_{2n+1} = 2, \forall n \in [N]$. In that case, it's clear that the support condition is violated. We note that $P(\mathsf{h}=1) = P(\mathsf{h}=2) = \frac{1}{2}$, $\mathscr{H} = \{1,2\}$, and thus $|\mathsf{h}|$ is not constant w.p. 1. However, by normalizing the odd symbols by factor $\frac{1}{2}$ we have $\mathsf{y}_n \perp\!\!\!\perp \mathsf{h}_n$, $\forall n \in [N]$ and the obfuscation constraint is satisfied. Then, any code optimized for a classical AWGN channel will achieve a positive rate, so the capacity is greater than zero. We note that the former proof breaks since, in this case, the support of h given u is not $\mathscr{H}$ anymore (since given u, h is deterministic).

Remark 9 (Strict Independence). If instead of (2.3) we require that $I\left(\mathsf{y}^N;\mathsf{h}^N\right) = 0, \forall N$, then this further implies that $I\left(\mathsf{y}_i;\mathsf{h}_i\right) = 0, \forall i \in [N]$ and similarly to the previous proofs we further have that $|\mathsf{h}_i|$ is constant w.p. 1 and the overall proof is simplified.

Building on Conj. 9, we now calculate the obfuscated capacity of the Gaussian channel with correlated fading. However, since the capacity will depend on the exact distribution of the variable h, we restrict our theorem to the case where $|\mathsf{h}_t| = \tilde{h}, \forall t \geq 1$. In that case, we note that $|\mathsf{h}| = \tilde{h}$.

Theorem 6. *The obfuscated capacity of the scalar Gaussian fading channel s.t.* $|\mathsf{h}_t| = \tilde{h}, \forall t \geq 1$ *is lower bounded by*

$$C_{\text{ob}} \geq \frac{1}{2}\log(\text{SNR}) \cdot (1 + o(1))$$

If furthermore $h\left(\angle\mathsf{h}\right) > -\infty$ *then*

$$C_{\text{ob}} = \frac{1}{2}\log(\text{SNR}) \cdot (1 + o(1))$$

Proof. For the lower bound, we use the same coding scheme from Th. 2. By the same reasoning as of Th. 2, it satisfies the obfuscation constraint and asymptotically attains the desired rate. This proves the lower bound. For the upper bound, we note that all the steps in the previous conjecture and lemma holds, where we do not need to assume about events hold w.p. 1 with regard to u. Thus, since in this case $|\mathsf{h}| = \tilde{h}$ w.p. 1, Lem. 9 tells us that the obfuscated capacity is upper bounded by that of the memoryless phase noise channel. Then, the upper bound follows using the results of [14, Sec. V]. □

4.2.2 Discussion

In general, the alphabet of auxiliary variables in information theory problems that involve continuous random variables is derived by taking limits of informational expressions over sequences of successively refined partitions of the continuous supports (see, for example, [13, Prop. 1]). Thus, we believe that Conj. 1 holds as a limit of a discretized setting (where the auxiliary alphabet can be derived via classical techniques [36, App. C]). Moreover, we note that our conjecture claims that $|\mathsf{h}|$ is constant w.p. 1, which is a weaker requirement than the one we made in Th. 6 (as one can allow to a finite number of elements to have a non-constant magnitude).

Chapter 5

The Obfuscated Capacity of the Discrete-Time ISI Gaussian Channel

In this chapter, we analyze the obfuscated capacity of the Gaussian ISI channel, defined in (2.2). To that end, we first review background material on circulant matrices and the discrete Fourier transform.

5.1 Circulant Matrices and Discrete Fourier Transform

This section reviews the concept of circulant matrices and the Discrete Fourier Transform (DFT).

Definition 1 (Circulant Matrix [38])**.** A matrix $\boldsymbol{H} \in \mathbb{C}^{n\times n}$ is called circulant if $\boldsymbol{H}[k,j] = h_{(j-k)_n}$, $(j,k) \in [n]$, for some sequence h^n. Here $(a)_n \triangleq a - n \cdot \lfloor \frac{a-1}{n} \rfloor$ denotes the modulo-n operation on a. The sequence h^n is called the generating sequence of $\boldsymbol{H}$.

Definition 2. The length-N DFT of a sequence a^n where $N \geq n$ is denoted by A^N and is defined via

$$A^N \triangleq \boldsymbol{F}_{N,n} a^n$$

where $\boldsymbol{F}_{N,n}$ is defined as $\boldsymbol{F}_{N,n}[l,k] = \frac{1}{\sqrt{N}} e^{j2\pi \frac{(l-1)(k-1)}{N}}$, $l \in [N], k \in [n]$ and is called the DFT matrix.[1] When $N = n$, we write $\boldsymbol{F}_n$ instead of $\boldsymbol{F}_{n,n}$.

Circulant matrices are known to be diagonalizable by DFT matrices, and their eigenvalues are the DFT of their generating sequence [38, Sec. 3.1]. Namely, let $\boldsymbol{H}$ be a circulant matrix generated by the sequence h^n, then

$$\boldsymbol{H} = \boldsymbol{F}_n^\dagger \mathrm{diag}\left(H^n\right) \boldsymbol{F}_n \tag{5.1}$$

where $H^n \triangleq \boldsymbol{F}_n h^n$.

[1] Here we use capital letters for variables in the frequency domain and lower-case letters for those in the time domain. To be consistent with the notation used throughout this paper, we start the indices from 1 and not 0.

5.2 The Obfuscated Capacity of the Circular ISI Channel

The circular-ISI channel is defined as

$$\mathsf{y}_n = \sum_{\ell=1}^{L} \mathsf{h}_\ell \mathsf{x}_{(n-\ell+1)_N} + \mathsf{z}_n,\ n = 1, \dots N$$

where $(x)_N \triangleq x - N \cdot \lfloor \frac{x-1}{N} \rfloor$. We analyze the following quantity, which we term *informational obfuscated capacity*, without discussing its operational meaning:

$$\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \{\mathsf{h}_\ell\}) \triangleq \lim_{N\to\infty} \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N)$$

where

$$\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N) \triangleq \sup_{\substack{P_{\mathsf{x}^N}: \\ \frac{1}{N}\sum_{n=1}^{N} \mathbb{E}[|\mathsf{x}_n|^2] \le 1}} \frac{1}{N} I\left(\mathsf{x}^N; \mathsf{y}^N\right), \quad \text{s.t. } I\left(\mathsf{y}^N; \mathsf{h}^L\right) = 0.$$

By viewing the outputs y^N as a single vector, we have

$$\mathsf{y}^N = \mathbf{H}\mathsf{x}^N + \mathsf{z}^N \tag{5.2}$$

where $\mathbf{H}$ is a circulant matrix generated from the sequence $\tilde{\mathsf{h}}^N \triangleq (\mathsf{h}_1, 0, \dots, 0, \mathsf{h}_L, \dots, \mathsf{h}_2)^T$ (recall Def. 1). Using (5.1) in (5.2) yield

$$\begin{aligned} \mathsf{y}^N &= \boldsymbol{F}_N^\dagger \text{diag}\left(\mathsf{H}^N\right) \boldsymbol{F}_N \mathsf{x}^N + \mathsf{z}^N \\ &\triangleq \boldsymbol{F}_N^\dagger \text{diag}\left(\mathsf{H}^N\right) \mathsf{X}^N + \mathsf{z}^N \end{aligned} \tag{5.3}$$

where $\mathsf{X}^N \triangleq \boldsymbol{F}_N \mathsf{x}^N$. Thus, after taking the DFT of the vector y^N this channel is transformed to

$$\mathsf{Y}^N = \text{diag}\left(\mathsf{H}^N\right) \mathsf{X}^N + \mathsf{Z}^N$$

where $\mathsf{Y}^N \triangleq \boldsymbol{F}_N \mathsf{y}^N$ and $\mathsf{Z}^N \triangleq \boldsymbol{F}_N \mathsf{z}^N$ is a zero-mean i.i.d. Gaussian vector with covariance $\frac{1}{\text{SNR}}\mathbf{I}_N$. This operation transformed the circular ISI channel into a set of N parallel scalar Gaussian channels.

Lemma 10. *The informational obfuscated capacity of the length-N circular Gaussian ISI channel, $\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N)$, satisfies*

$$\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N) \ge \frac{|\mathcal{F}|}{2N} \cdot \log(\text{SNR}) \cdot (1 + o(1)) \tag{5.4}$$

where $\mathcal{F} \triangleq \{k : \ |\mathsf{H}_k| = |H_k| > 0 \text{ constant w.p. } 1\}$. Furthermore, (5.4) holds with equality if

$$h\left(\{\angle \mathsf{H}_i\}_{i\in\mathcal{F}}\right) > -\infty. \tag{5.5}$$

Proof. Since the channel is a circular convolution channel and since the noise is Gaussian, by using the data-processing inequality, we get

$$\begin{aligned}
&\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N) \\
&= \sup_{\substack{P_{\mathsf{x}^N}: \\ \frac{1}{N}\sum_{n=1}^N \mathbb{E}[|\mathsf{x}_n|^2] \le 1}} \frac{1}{N} I\left(\mathsf{x}^N; \mathsf{y}^N\right) \text{ s.t. } I\left(\mathsf{h}^L; \mathsf{y}^N\right) = 0 \\
&= \sup_{\substack{P_{\mathsf{X}^N}: \\ \frac{1}{N}\sum_{n=1}^N \mathbb{E}[|\mathsf{x}_n|^2] \le 1}} \frac{1}{N} I\left(\mathsf{X}^N; \mathsf{Y}^N\right) \text{ s.t. } I\left(\mathsf{h}^L; \mathsf{y}^N\right) = 0 \qquad (5.6) \\
&= \sup_{\substack{P_{\mathsf{X}^N}: \\ \frac{1}{N}\sum_{n=1}^N \mathbb{E}[|\mathsf{x}_n|^2] \le 1}} \frac{1}{N} I\left(\mathsf{X}^N; \mathsf{Y}^N\right) \text{ s.t. } I\left(\mathsf{H}^N; \mathsf{Y}^N\right) = 0 \qquad (5.7)
\end{aligned}$$

where (5.6) is by defining $\mathsf{X}^N \triangleq \boldsymbol{F}_N \mathsf{x}^N$ and $\mathsf{Y}^N \triangleq \boldsymbol{F}_N \mathsf{y}^N$ and by using the Gaussianity of the noise in the channel (5.3) and the fact that the average mutual information between two sequences is invariant to any succession of reversible transformations of one or both of the sequences [39, P. 30-31]; and (5.7) is by defining the transformed version of h^L, $\mathsf{H}^N = \boldsymbol{F}_{N,L} \mathsf{h}^L$ and by using the invariance of the mutual information to reversible transformations; We first prove the lower bound by evaluating (5.7) for a specific choice of the input distribution. To that end, for all indices $i \in [N]$ s.t. $|\mathsf{H}_i|$ is constant w.p. 1 we suggest picking $\mathsf{X}_i = \sqrt{P_i}\tilde{\mathsf{X}}_i$ where $\tilde{\mathsf{X}}_i$ are i.i.d. and distributed according to the input distribution as in the achievability part of Th. 2 and where the P_i are s.t. $\frac{1}{N}\sum_{i=1}^N P_i \le 1$. For all the other indices, we set $\mathsf{X}_i = 0$. Since the $\{\mathsf{X}_i\}$ are i.i.d. we have $\frac{1}{N} I\left(\mathsf{X}^N; \mathsf{Y}^N\right) = \frac{1}{N}\sum_{i=1}^N I\left(\mathsf{X}_i; \mathsf{Y}_i\right)$, and by Th. 2 we further have $I\left(\mathsf{X}_i; \mathsf{Y}_i\right) = \frac{1}{2}\log\left(P_i \cdot \text{SNR}\right) \cdot (1 + o(1))$ and $I\left(\mathsf{H}^N; \mathsf{Y}^N\right) = 0$. Thus, the obfuscation constraint is satisfied, and the mutual information $\frac{1}{N} I\left(\mathsf{X}^N; \mathsf{Y}^N\right)$ attained with this scheme is given by

$$\begin{aligned}
\frac{1}{N} I\left(\mathsf{X}^N; \mathsf{Y}^N\right) &= \sup_{\substack{\sum_{k=1}^N P_k \le N \\ P_k \ge 0, \forall k \in [N]}} \sum_{k \in \mathcal{F}} \frac{1}{2N} \log\left(P_k \cdot \text{SNR}\right)(1 + o(1)) \\
&= \frac{|\mathcal{F}_N|}{2N} \cdot \log\left(\text{SNR}\right) \cdot (1 + o(1)) \qquad (5.8)
\end{aligned}$$

where $\mathcal{F}_N$ is the subset of $k \in [N]$ s.t. $|\mathsf{H}_k|$ is constant w.p. 1 and non-zero.

To upper bound (5.7), we first note that $I\left(\mathsf{H}^N; \mathsf{Y}^N\right) = 0$ implies $\mathsf{H}_i \perp\!\!\!\perp \mathsf{Y}_i, \forall i \in [N]$. Thus,

we get

$$\begin{aligned}\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR},\mathsf{h}^L,N) &= \sup_{\substack{P_{\mathsf{X}^N}:\\ \frac{1}{N}\sum_{n=1}^{N}\mathbb{E}[|\mathsf{x}_n|^2]\le 1}} \frac{1}{N} I\left(\mathsf{X}^N;\mathsf{Y}^N\right) \text{ s.t. } I\left(\mathsf{H}^N;\mathsf{Y}^N\right)=0 \\ &\le \sup_{\substack{P_{\mathsf{X}^N}:\\ \frac{1}{N}\sum_{k=1}^{N}\mathbb{E}\left[|\mathsf{x}_k|^2\right]\le 1}} \frac{1}{N} I\left(\mathsf{X}^N;\mathsf{Y}^N\right) \text{ s.t. } I\left(\mathsf{H}_k;\mathsf{Y}_k\right)=0, \forall k\in[N] \\ &\le \sup_{\substack{P_{\{\mathsf{x}_i\}_{i\in\mathcal{F}_N}}:\\ \frac{1}{N}\sum_{k\in\mathcal{F}_N}\mathbb{E}\left[|\mathsf{x}_k|^2\right]\le 1}} \frac{1}{N} I\left(\{\mathsf{X}_i\}_{i\in\mathcal{F}_N};\{\mathsf{Y}_i\}_{i\in\mathcal{F}_N}\right) \end{aligned} \tag{5.9}$$

where the last step is by using Th. 2, which tells us that for any $i\notin\mathcal{F}_N$ we must set $\mathsf{X}_i=0$ to not violate the obfuscation constraint. We note that (5.9) is equivalent to the capacity of the MIMO phase noise channel with transmitter phase-noise as defined in [40], and thus by [40, Sec. I.B] its capacity is given by (5.8) whenever $h\left(\{\angle\mathsf{H}_i\}_{i\in\mathcal{F}_N}\right)>-\infty$.

□

We note that the proof of Lem. 10 is by reducing the length-N informational obfuscated capacity of the circular ISI channel to a sum of $|\mathcal{F}_N|$ arguments, which we can then evaluate by Th. 2. This relation extends a classical result in communication, relating the (classical, without obfuscation constraint) circular ISI channel to a set of parallel scalar Gaussian channels [11]. However, the obfuscation constraint limits our communication to frequencies over which the channel frequency response $\mathsf{H}(f)$ has a constant magnitude (w.p. 1). This is in contrast to the classical ISI channel, where communication can be done at any frequency for which $|\mathsf{H}(f)|>0$.

We now evaluate the informational obfuscated capacity of the circular ISI channel, $\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR},\{\mathsf{h}_\ell\})$, by calculating the limit $\lim_{N\to\infty}\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR},\mathsf{h}^L,N)$. To that end, we make the next definitions

$$\mathscr{W}\triangleq\{f\in[0,1)\colon |\mathsf{H}(f)|>0 \text{ and constant w.p. } 1\},\ W\triangleq\int_0^1 \mathbb{1}\{f\in\mathscr{W}\}\,df \tag{5.10}$$

and we assume that $\mathscr{W}$ is a measurable set.

Lemma 11. *The informational obfuscated capacity of the circular ISI channel is lower bounded by*

$$\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR},\{\mathsf{h}_\ell\})\ge\frac{W}{2}\cdot\log(\text{SNR})\cdot(1+o(1)) \tag{5.11}$$

Furthermore, (5.11) *holds with equality if*

$$h\left(\{\angle\mathsf{H}(f_i)\}_{i=1}^m\right)>-\infty \tag{5.12}$$

for any $m\ge 1$ and any sequence of frequencies $\{f_i\}_{i=1}^m$ s.t. $f_i\in\mathscr{W},\forall i\in[m]$.

Proof. The proof is by evaluating the limit $\lim_{N\to\infty} \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N)$ from Lem. 10. For any finite N, we define the next set of frequencies $\left\{f_k = \frac{k}{N}\right\}_{k=0}^{N-1}$ and $\Delta_N \triangleq \frac{1}{N}$. We note that

$$\frac{|\mathcal{F}_N|}{N} = \frac{1}{N}\sum_{k=0}^{N-1} \mathbb{1}\left\{\left|\mathsf{H}_L\left(f = \frac{k}{N}\right)\right| > 0 \text{ and constant w.p. } 1\right\} \underset{N\to\infty}{\longrightarrow} W$$

where the limit is since $\mathscr{W}$ is a measurable set and by using the Lesbegue integral. Thus, we note that (5.8) converges to (5.11). Moreover, the converse result of Lem. 10 suggests that this lower bound is tight (up to terms which are $o(1)$ with the SNR), as long as $\lim_{N\to\infty} h\left(\left\{\angle \mathsf{H}_L\left(f = \frac{i}{N}\right)\right\}_{i\in\mathcal{F}_N}\right) > -\infty$. As $N \to \infty$, we note that this suggests that the differential entropy of any finite-dimensional distribution of the phase process $\{\angle \mathsf{H}(f), f \in \mathscr{W}\}$ is finite, similarly to our definition of (5.12). □

5.3 The Obfuscated Capacity of the Regular ISI Channel

We now analyze the obfuscated capacity of the regular Gaussian ISI channel (2.2). We define the *informational obfuscated capacity* as

$$\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\}) \triangleq \lim_{N\to\infty} \bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \mathsf{h}^L, N) \tag{5.13}$$

where

$$\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \mathsf{h}^L, N) \triangleq \sup_{\substack{P_{\mathsf{x}^N}: \\ \frac{1}{N}\sum_{n=1}^{N}\mathbb{E}[|\mathsf{x}_n|^2]\le 1}} \frac{1}{N} I\left(\mathsf{x}^N; \mathsf{y}^N\right) \text{ s.t. } I\left(\mathsf{y}_L^N; \mathsf{h}^L\right) = 0$$

We start by adapting a classical result of Gallager to connect (5.13) to the operational obfuscated capacity. We then prove that $\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\}) = \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \{\mathsf{h}_\ell\})$.

Lemma 12. *The obfuscated capacity of the regular ISI channel is given by* $C_{\text{ob}}(\text{SNR}) = \bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\})$.

Proof Sketch. The proof follows by using [39, Sec. 4.6] and [39, Sec. 5.9], which, since x_{-L+1}^0 is constant, claims that for any fixed input distribution P_{x^N} we can communicate with vanishing probability of error as long as $R < \lim_{N\to\infty} \frac{1}{N} I\left(\mathsf{x}^N; \mathsf{y}^N\right)$, where otherwise reliable communication is impossible[2]. For the achievability, the codewords are generated by sampling uniformly $2^{\lfloor NR \rfloor}$ vectors from P_{x^N}, denoted by $\left\{u^N(M)\right\}_{M=1}^{\lfloor 2^{NR}\rfloor}$. We denote by u^N a variable whose distribution is the same as that of every $u^N(M)$. The power constraint is satisfied as $N \to \infty$ by the classical arguments. Moreover, by the obfuscation constraint and since the codebook

[2]Since the original proof requires that L will be finite for any N and that $\lim_{N\to\infty} \frac{L}{N} = 0$ this holds also for the case where $L = o(N)$

is generated without CSI, then $P_{\mathsf{y}_L^N,\mathsf{u}^N|\mathsf{h}^L}(y_L^N,u^N|h^L)=P_{\mathsf{y}_L^N,\mathsf{u}^N}(y_L^N,u^N)$. Thus,

$$\begin{aligned}
&P_{\mathsf{y}_L^N,\mathsf{h}^L}\left(y_L^N,h^L\right)\\
&=P_{\mathsf{h}^L}\left(h^L\right)\left(\sum_{M=1}^{2^{\lfloor NR\rfloor}}P_{\mathsf{y}_L^N,\mathsf{u}^N|\mathsf{h}^L}\left(y_L^N,u^N(M)|h^L\right)\right)\\
&=P_{\mathsf{h}^L}\left(h^L\right)\left(\sum_{M=1}^{2^{\lfloor NR\rfloor}}P_{\mathsf{y}_L^N,\mathsf{u}^N}\left(y_L^N,u^N(M)\right)\right)\\
&=P_{\mathsf{h}^L}\left(h^L\right)P_{\mathsf{y}_L^N}\left(y_L^N\right)
\end{aligned}$$

Thus, this choice satisfies the obfuscation constraint. The supremum of R over P_{x^N} under the power constraint and the obfuscation constraint is given by $\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR},\{\mathsf{h}_\ell\})$ and further equals the obfuscated capacity. □

Theorem 7. *The obfuscated capacity of the regular ISI channel (2.2) satisfies*

$$C_{\text{ob}}(\text{SNR})\geq\frac{W}{2}\cdot\log(\text{SNR})\cdot(1+o(1)),\tag{5.14}$$

where W is defined in (5.10). Furthermore, (5.14) holds with equality if (5.12) is satisfied.

Proof. The proof evaluates (5.13) by first looking at a finite N, and proving an upper and a lower bound on $\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR},\mathsf{h}^L,N)$. Then, we show that as $N\to\infty$ the bounds converge to those of Lem. 10.

Upper Bound: We look at an ISI channel with $N+L$ channel outputs and define the next set of input distributions

$$\mathscr{P}_U\triangleq\left\{P_{\mathsf{x}^{N+L}}:\ \mathsf{x}_{N+1}^{N+L}=0,\ \frac{\mathbb{E}\left[\left\|\mathsf{x}^{N+L}\right\|^2\right]}{N+L}\leq 1\right\}$$

We note that $\mathscr{P}_U$ contains all the possible input distributions for the length-N ISI channel. Let

$$R^{\text{reg}}(\mathsf{x}^N,\mathsf{y}_l^k)\triangleq\frac{1}{k-l+1}I\left(\mathsf{x}^N;\mathsf{y}_l^k\right)$$

for the ISI channel and similarly define $R^{\text{circ}}(\mathsf{x}^N,\mathsf{y}_l^k)$ for the circular case. Then,

$$\begin{aligned}
\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR},\mathsf{h}^L,N)&\leq\max_{\substack{P_{\mathsf{x}^{N+L}}\in\mathscr{P}_U:\\ I\left(\mathsf{y}_L^N;\mathsf{h}^L\right)=0}}\frac{N+L}{N}\cdot R^{\text{reg}}\left(\mathsf{x}^{N+L},\mathsf{y}^{N+L}\right) &(5.15)\\
&=\max_{\substack{P_{\mathsf{x}^{N+L}}\in\mathscr{P}_U:\\ I\left(\mathsf{y}_L^N;\mathsf{h}^L\right)=0}}\frac{N+L}{N}\cdot R^{\text{circ}}\left(\mathsf{x}^{N+L},\mathsf{y}^{N+L}\right) &(5.16)\\
&\leq\max_{\substack{P_{\mathsf{x}^{N+L}}\\ \frac{1}{N+L}\mathbb{E}\left[\|\mathsf{x}^{N+L}\|^2\right]\leq 1\\ I\left(\mathsf{y}_L^N;\mathsf{h}^L\right)=0}}\frac{N+L}{N}\cdot R^{\text{circ}}\left(\mathsf{x}^{N+L},\mathsf{y}^{N+L}\right) &(5.17)
\end{aligned}$$

where (5.15) is by the definition of $\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \mathsf{h}^L, N)$; (5.16) holds since the linear and circular convolution yields the same output sequence y^{N+L} for any input distribution in $\mathscr{P}_U$; and (5.17) holds since we are not limiting the input distribution to be in $\mathscr{P}_U$. We denote the columns L-to-N of the matrix $\boldsymbol{F}_{N+L}$ (defined in Def. 2) by $\boldsymbol{F}_{N+L,(L:N)}$. Then,

$$\mathsf{y}_L^N = \boldsymbol{F}_{N+L,(L:N)}^{\dagger} \text{diag}\left(\mathsf{H}^{N+L}\right) \mathsf{X}^{N+L} + \mathsf{z}_L^N$$

where $\mathsf{H}^{N+L} \triangleq \boldsymbol{F}_{N+L,L}\mathsf{h}^L$. By the invariance of the MI to reversible transformations, we note that $I\left(\mathsf{y}_L^N; \mathsf{h}^L\right) = 0$ implies $I\left(\mathsf{y}_L^N; \mathsf{H}^{N+L}\right) = 0$. However, as $N \to \infty$, the matrix $\boldsymbol{F}_{N+L,(L:N)}^{\dagger}$ is invertible, and by the invariance of the MI to reversible transformations and Lem. 5 we get that as $N \to \infty$ the constraint $I\left(\mathsf{Y}_L^N; \mathsf{H}^{N+L}\right) = 0$ implies

$$\text{diag}\left(\mathsf{H}^{N+L}\right) \mathsf{X}^{N+L} \perp\!\!\!\perp \mathsf{H}^{N+L} \tag{5.18}$$

Substituting (5.18) in (5.17) and taking $N \to \infty$ yields

$$\begin{aligned}\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\}) \leq \lim_{N\to\infty} \sup_{\substack{P_{\mathsf{x}^{N+L}}: \\ \frac{1}{N+L}\sum_{n=1}^{N+L}\mathbb{E}[|\mathsf{x}_n|^2]\leq 1}} & \frac{N+L}{N}\frac{1}{N+L} I\left(\mathsf{x}^{N+L}; \mathsf{y}^{N+L}\right) \\ & \text{s.t. } I\left(\mathsf{H}_i\mathsf{X}_i; \mathsf{H}_i\right) = 0, \forall i \in [N+L] \\ = \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \{\mathsf{h}_\ell\}) &\end{aligned} \tag{5.19}$$

where the last equality is by the proof of Lem. 10.

Lower Bound: We look at an ISI channel of length $N+L$, for which we define the next set of input distributions

$$\mathscr{P}_L \triangleq \left\{ P_{\mathsf{x}^{N+L}} : \mathsf{x}_n = \mathsf{x}_{n+N}, \forall n \in [L], \quad \frac{\mathbb{E}\left[\left\|\mathsf{x}^{N+L}\right\|^2\right]}{N+L} \leq 1 \right\}$$

Since $\mathscr{P}_L$ is a subset of the possible input distributions $P_{\mathsf{x}^{N+L}}$ under the input power constraint we have:

$$\begin{aligned}\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \mathsf{h}^L, N+L) &\geq \max_{\substack{P_{\mathsf{x}^{N+L}} \in \mathscr{P}_L: \\ I\left(\mathsf{y}_L^{N+L}; \mathsf{h}^L\right)=0}} R^{\text{reg}}\left(\mathsf{x}^{N+L}, \mathsf{y}^{N+L}\right) \\ &\geq \max_{\substack{P_{\mathsf{x}^{N+L}} \in \mathscr{P}_L: \\ I\left(\mathsf{y}_L^{N+L}; \mathsf{h}^L\right)=0}} R^{\text{reg}}\left(\mathsf{x}^{N+L}, \mathsf{y}_L^{N+L}\right) && (5.20) \\ &= \max_{\substack{P_{\mathsf{x}_{L+1}^{N+L}} \\ \frac{1}{N}\sum_{t=L+1}^{N+L}\mathbb{E}[|\mathsf{x}_n|^2]\leq 1 \\ I\left(\mathsf{y}_L^{N+L}; \mathsf{h}^L\right)=0}} R^{\text{circ}}\left(\mathsf{x}_{L+1}^{N+L}, \mathsf{y}_L^{N+L}\right) && (5.21) \\ &= \max_{\substack{P_{\mathsf{x}^N} \\ \frac{1}{N}\sum_{n=1}^{N}\mathbb{E}[|\mathsf{x}_n|^2]\leq 1 \\ I\left(\mathsf{y}^N; \mathsf{h}^L\right)=0}} R^{\text{circ}}\left(\mathsf{x}^N, \mathsf{y}^N\right) && (5.22) \\ &= \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N) && (5.23)\end{aligned}$$

where (5.20) holds by the chain rule; (5.21) holds since the linear and circular convolution yields the same output sequence y_L^{N+L} for any input distribution in $\mathscr{P}_L$; (5.22) holds since the mutual information is time-invariant; and (5.23) is by the definition of $\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \mathsf{h}^L, N)$. Taking $N \to \infty$ yields $\bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\}) \geq \bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \{\mathsf{h}_\ell\})$. Combining (5.19) and (5.23) yields $\bar{C}_{\text{ob}}^{\text{circ}}(\text{SNR}, \{\mathsf{h}_\ell\}) = \bar{C}_{\text{ob}}^{\text{reg}}(\text{SNR}, \{\mathsf{h}_\ell\})$. Then, the proof follows by combining Lem. 10 and Lem. 12. □

Remark 10 (ISI Multiplexing-Gain). Denote $W_p \triangleq \int_0^1 \mathbb{1}\{f : |\mathsf{H}(f)| > 0, \text{ w.p. } 1\}\, df$. By Th. 7, if (5.5) is true, then the multiplexing gain of the obfuscated capacity is reduced by a factor of $W/(2W_P)$ relative to that of the classical ISI channel [11].

5.3.1 Discussion

The obfuscated capacity we calculated depends on $\mathscr{W}$ and W as defined in (5.10). Here, W represents the overall frequency band where the frequency response magnitude is positive and deterministic with probability 1. The obfuscated capacity becomes zero whenever $W = 0$. However, since the channel frequency response is completely characterized by $\{\mathsf{h}_\ell\}_{\ell=1}^L$ from (2.2), it is unclear if we can simultaneously satisfy (5.12) while having $W > 0$. Consequently, whether there exists a set of physical channel models for which Th. 7 precisely characterizes the obfuscated capacity remains an open question.

Chapter 6

Conclusion and Future Work

In this work, we analyzed the obfuscated capacity of multiple scalar fading Gaussian channel variants and calculated their asymptotic value in a closed form. We further presented communication strategies for each variant that asymptotically attain the capacity. We note that, for the case of quasistatic fading, we derived a single-letter upper bound on the obfuscated capacity and on the obfuscated capacity with feedback, which was proved to be asymptotically tight. However, such a result does not hold for general channels, and finding such a single-letter expression for the obfuscated capacity is an interesting direction for future research. Moreover, for the correlated fading, we could evaluate the upper bound only under specific assumptions on the channel coefficients. Evaluating this bound in the general case is another possible venue for future research. Our analysis only considered the single-antenna case. The multiple-antenna case is another interesting direction that is under investigation.

Appendix A

Alternative Proof of Lem. 6

We now provide an alternative proof to Lem. 6. We note that this proof does not require any assumptions on the second moments of h not x.

Lemma 13. *Let* a *and* d *be nonnegative-valued random variables satisfying* $\mathsf{a} \perp\!\!\!\perp \mathsf{d}$, $\mathsf{da} \perp\!\!\!\perp \mathsf{a}$, *and* $P(\mathsf{a} > 0, \mathsf{d} > 0) > 0$. *Then, we must have that* a *is almost surely constant.*

Proof. Assume for the sake of contradiction that a is not almost surely constant, so we have that there exists some a_0 satisfying $0 < P(\mathsf{a} \leq a_0) < 1$. By right-continuity of CDFs, we have that there exists some $\varepsilon > 0$ such that $P(\mathsf{a} \leq a_0 + 2\varepsilon) < 1$. Then, choose d_0 to satisfy the property that

$$P\left(\mathsf{d} \in \left(\frac{a_0+\varepsilon}{a_0+2\varepsilon}d_0, \frac{a_0+\varepsilon}{a_0}d_0\right)\right) > 0$$

Using independence of a and d we obtain that

$$P(\mathsf{da} \leq (a_0+\varepsilon)d_0 | \mathsf{a} \leq a_0) = P\left(\mathsf{d} \leq \frac{a_0+\varepsilon}{\mathsf{a}}d_0 \middle| \mathsf{a} \leq a_0\right) \geq P\left(\mathsf{d} \leq \frac{a_0+\varepsilon}{a_0}d_0\right)$$

and similarly

$$P(\mathsf{da} \leq (a_0+\varepsilon)d_0 | \mathsf{a} > a_0 + 2\varepsilon) \leq P\left(\mathsf{a} < \frac{a_0+\varepsilon}{a_0+2\varepsilon}d_0\right).$$

By our choice of d_0 we have that these two probabilities are not equal, and by our choice of a_0 we have that the events $\mathsf{a} \leq a_0$ and $\mathsf{a} > a_0 + 2\varepsilon$ happen with nonzero probability. Then $\mathsf{da} \not\perp\!\!\!\perp \mathsf{d}$, which is a contradiction, so we conclude that a must be constant almost surely. The proof of Lem. 6 follows by using $\mathsf{a} = |\mathsf{h}|$ and $\mathsf{d} = |\mathsf{x}|$. □

Appendix B

Background on the Dirty-Paper Channel

We now provide background on the problem of dirty-paper (DP) channel and its connection to state-masking.

The dirty-paper (DP) channel, first introduced by Costa [19], provides an information-theoretic framework for the study of interference cancellation techniques for interference known to the transmitter. The DP channel model has since been further studied and applied to different communication scenarios such as ISI channels [21], the MIMO Gaussian broadcast channel [26], the MIMO multiple-access channel [41], information embedding [42], [43], and have been proved useful as a building block in a joint source-channel coding system [44]. In the additive Gaussian case, the DP channel is

$$\mathsf{y}_t = \mathsf{x}_t + \mathsf{s}_t + \mathsf{z}_t,\ t = 1, \ldots, N$$

and is composed of an input signal x_t, subject to a power constraint, corrupted by additive white Gaussian noise (AWGN) z_t and additive interference s_t which is known to the transmitter but not to the receiver, causally ("causal DP") $\mathsf{x}_i = \phi\left(\mathsf{M}, \mathsf{s}^i\right)$ or non-causally ("non-causal DP") $\mathsf{x}_i = \phi\left(\mathsf{M}, \mathsf{s}^n\right)$ where M is the transmitted message, ϕ is a function satisfying the input constraint and x_i and s_i are the channel input and interference at time instance $i,\ 1 \leq i \leq n$, respectively.

Costa [19] showed that, for an i.i.d. Gaussian interference with arbitrary power, the capacity in the non-causal scenario is equal to that of the interference-free AWGN channel. This result was extended in [45] to the case of general ergodic interference and to arbitrary interference in [22]. The capacity of the DP channel with causal knowledge of the interference, first considered by Willems [46], is not known but upper and lower bounds for the case of arbitrary interference were found in [22], which coincide in the high SNR regime, thus establishing the capacity for this case to be the same as for the interference-free AWGN channel (or equivalently for the non-causal DP channel) up to a shaping loss. Thus, causality incurs a rate loss of $\frac{1}{2}\log\left(\frac{2\pi e}{12}\right)$ relative to the capacity of the interference-free AWGN channel, in the high SNR regime. This result implies that in the limit of strong interference and high SNR, the well-known Tomlinson-Harashima precoding (THP) technique [21] is optimal. For general SNRs, the lattice-based coding techniques of [22], [43] are an extension of Tomlinson-Harashima precoding, sometimes referred to as MMSE (minimum mean-square error) Tomlinson-Harashima precoding, where a scaling parameter is introduced at the transmitter and receiver. Similar schemes have been proved useful in the case where the SNR is

unknown [25]. The causal and non-causal DP channels are special cases of the problem of a general state-dependent memoryless channel. This problem was first introduced by Shannon in 1958 [17], who found the capacity for the case of a causally known state. Kuznetzov and Tsybakov considered the non-causal scenario [47], the general capacity of which was found by Gel'fand and Pinsker in 1980 [18].

References

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Comm.*, vol. 17, no. 5, pp. 56–62, 2010.

[2] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE IoT. Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[3] M. Cominelli, F. Gringoli, and R. L. Cigno, "On the properties of device-free multi-point CSI localization and its obfuscation," *Computer Communications*, vol. 189, pp. 67–78, 2022.

[4] L. F. Abanto-Leon, A. Bäuml, G. H. Sim, M. Hollick, and A. Asadi, "Stay connected, leave no trace: Enhancing security and privacy in WiFi via obfuscating radiometric fingerprints," *Proc. of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 3, pp. 1–31, 2020.

[5] M. Cominelli, F. Kosterhon, F. Gringoli, R. Lo Cigno, and A. Asadi, "IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios," *Computer Networks*, vol. 191, p. 107 970, 2021, ISSN: 1389-1286.

[6] M. Cominelli, F. Gringoli, and R. L. Cigno, "Antisense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing," *Computer Communications*, vol. 185, pp. 92–103, 2022.

[7] L. Ghiro, M. Cominelli, F. Gringoli, and R. Lo Cigno, "Wi-fi localization obfuscation: An implementation in openwifi," *Computer Communications*, May 2023.

[8] H. Givehchian, N. Bhaskar, A. Redding, H. Zhao, A. Schulman, and D. Bharadia, "Practical obfuscation of BLE physical-layer fingerprints on mobile devices," in *2024 IEEE Symposium on Security and Privacy (SP)*, IEEE Computer Society, 2023, pp. 73–73.

[9] R. Ayyalasomayajula, A. Arun, W. Sun, and D. Bharadia, "Users are closer than they appear: Protecting user location from WiFi APs," in *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, 2023, pp. 124–130.

[10] L. Wang and G. W. Wornell, "Communication subject to state obfuscation," in *the International Zurich Seminar on Communication (IZS)*, ETH Zurich, 2020, pp. 78–82.

[11] W. Hirt and J. Massey, "Capacity of the discrete-time Gaussian channel with intersymbol interference," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 38–38, 1988. DOI: 10.1109/18.6015.

[12] S. Shamai and R. Laroia, "The intersymbol interference channel: Lower bounds on capacity and channel precoding loss," *IEEE Trans. Inf. Theory*, vol. IT-42, pp. 1388–1404, Sep. 1996.

[13] N. Merhav and S. Shamai, "Information rates subject to state masking," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2254–2261, 2007.

[14] A. Lapidoth, "On phase noise channels at high SNR," in *Proc. IEEE Info. Theory Workshop (ITW)*, 2002, pp. 1–4. DOI: 10.1109/ITW.2002.1115399.

[15] M. R. Khanzadi, G. Durisi, and T. Eriksson, "Capacity of SIMO and MISO phase-noise channels with common/separate oscillators," *IEEE Trans. Comm.*, vol. 63, no. 9, pp. 3218–3231, 2015. DOI: 10.1109/TCOMM.2015.2408605.

[16] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inf. Theory*, vol. 44, pp. 2148–2177, 1998.

[17] C. E. Shannon, "Channels with side information at the transmitter," *IBM Journal of Research and Development*, vol. 2, pp. 289–293, Oct. 1958.

[18] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Problemy Pered. Info. (Problems of Info. Trans.)*, vol. 9, No. 1, pp. 19–31, 1980.

[19] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[20] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacity of a class of channels," *The Annals of Math. Stat.*, vol. 30, pp. 1229–1241, Dec. 1959.

[21] M. Tomlinson, "New automatic equalizer employing modulo arithmetic," *Electronics Let.*, vol. 7, no. 5, pp. 138–139, Mar. 1971.

[22] U. Erez, S. Shamai, and R. Zamir, "Capacity and lattice strategies for canceling known interference," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3820–3833, Nov. 2005.

[23] U. Erez and S. ten Brink, "A close-to-capacity dirty paper coding scheme," *IEEE Trans. Inf. Theory*, vol. IT-51, pp. 3417–3432, Oct. 2005.

[24] A. Khisti, U. Erez, A. Lapidoth, and G. W. Wornell, "Carbon copying onto dirty paper," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1814–1827, 2007.

[25] A. Khina and U. Erez, "On the robustness of dirty paper coding," *IEEE Trans. Comm.*, vol. 58, no. 5, pp. 1437–1446, 2010.

[26] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[27] U. Pereg, C. Deppe, and H. Boche, "Quantum channel state masking," *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2245–2268, 2021.

[28] U. Pereg, C. Deppe, and H. Boche, "Classical state masking over a quantum channel," *Phys. Rev. A*, vol. 105, p. 022 442, 2 Feb. 2022.

[29] M. Ahmadipour, M. Wigger, and S. Shamai, "Integrated communication and receiver sensing with security constraints on message and state," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, IEEE, 2023, pp. 2738–2743.

[30] K. Kittichokechai, T. J. Oechtering, M. Skoglund, and Y.-K. Chia, "Secure source coding with action-dependent side information," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6444–6464, 2015.

[31] K. Tutuncuoglu, O. Ozel, A. Yener, and S. Ulukus, "State amplification and state masking for the binary energy harvesting channel," in *Proc. IEEE Info. Theory Workshop (ITW)*, IEEE, 2014, pp. 336–340.

[32] Y. Bu, T. Wang, and G. W. Wornell, "SDP methods for sensitivity-constrained privacy funnel and information bottleneck problems," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, IEEE, 2021, pp. 49–54.

[33] A. Shah, M. Shen, J. J. Ryu, S. Das, P. Sattigeri, Y. Bu, and G. W. Wornell, "Group fairness with uncertainty in sensitive attributes," *arXiv preprint arXiv:2302.08077*, 2023.

[34] R. Nuriyev and A. Anastasopoulos, "Capacity and coding for the block-independent noncoherent awgn channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 866–883, 2005.

[35] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York, NY: McGraw-Hill, 1965.

[36] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[37] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge University Press, 2014.

[38] R. M. Gray *et al.*, "Toeplitz and circulant matrices: A review," *Foundations and Trends® in Communications and Information Theory*, vol. 2, no. 3, pp. 155–239, 2006.

[39] R. G. Gallager, *Information Theory and Reliable Communication*. New York: John Wiley & Sons, 1968.

[40] S. Yang and S. S. Shitz, "On the multiplexing gain of discrete-time MIMO phase noise channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2394–2408, 2017.

[41] A. Khina, Y. Kochman, and U. Erez, "The dirty MIMO multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 6031–6040, 2017.

[42] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1159–1180, May 2003.

[43] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inf. Theory*, vol. IT–47, pp. 1423–1443, May 2001.

[44] Y. Kochman and R. Zamir, "Joint Wyner-Ziv/dirty-paper coding by modulo-lattice modulation," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4878–4899, Nov. 2009.

[45] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1639–1667, Jun. 2002.

[46] F. M. J. Willems, "On Gaussian channels with side information at the transmitter," in *Proc. of the Ninth Symposium on Information Theory in the Benelux*, Enschede, The Netherlands, 1988.

[47] A. V. Kuznetsov and B. S. Tsybakov, "Coding in a memory with defective cells," *translated from Prob. Peredach. Info.*, vol. 10, pp. 52–60, April-June, 1974.