Soft Covering Through the Lens of Hypothesis Testing

Neri Merhav

May 19, 2026

The Viterbi Faculty of Electrical and Computer Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 3200003, ISRAEL
E–mail: merhav@technion.ac.il

Abstract

The soft covering lemma asserts that a random codebook whose rate R exceeds the input-output mutual information, $I(X;Y)$, of a given discrete memoryless channel (DMC), causes the output mixture distribution to be statistically indistinguishable from the i.i.d. output distribution. We study this phenomenon through the lens of Neyman–Pearson hypothesis testing: given a channel output sequence y^n, can one decide whether it was produced when the channel was driven by a random codeword, or generated independently from the output marginal? We derive exact exponential decay rates for the jointly averaged false-alarm (FA) probability $\alpha_n(\tau, R)$ and missed-detection (MD) probability $\beta_n(\tau, R)$, as functions of the decision threshold τ and the codebook rate R. The derived single-letter formulas of the exponents $E_{\rm FA}(\tau, R) = -\lim_{n\to\infty} \frac{1}{n} \ln \alpha_n(\tau, R)$ and $E_{\rm MD}(\tau, R) = -\lim_{n\to\infty} \frac{1}{n} \ln \beta_n(\tau, R)$ are tight in the random coding sense. The analysis reveals a rich phase structure. For $R < I(X;Y)$, there is a genuine exponential tradeoff between the two error types over the interval $\tau \in (0, I(X;Y) - R)$. At $R = I(X;Y)$, this tradeoff interval collapses to the single point $\tau = 0$, where both error exponents simultaneously vanish, a fact which manifests the soft covering phenomenon in the Neyman–Pearson sense. For $R > I(X;Y)$, the same instantaneous collapse persists at $\tau = 0$; moreover, for every τ at least one exponent is zero: the FA exponent is zero for $\tau \le 0$ (FA probability does not decay exponentially), and the MD exponent is zero for $\tau \ge 0$ (and finite, channel-specific for $\tau < 0$; see Remark 1). There is no interval of τ where both exponents are simultaneously positive. A sharp phase transition in the MD exponent occurs at $\tau^* = [I(X;Y) - R]_+$ for all rates.

Index Terms: soft covering, hypothesis testing, error exponents, phase transitions.

1 Introduction

The soft covering lemma, introduced by Han and Verdú [1], is a cornerstone of information theory. It asserts that a random codebook $\mathcal{C}$ of rate $R > I(X;Y)$ causes the channel output mixture distribution $P_{Y^n|\mathcal{C}}$ to become statistically indistinguishable from the i.i.d. output distribution $P_Y^{\otimes n}$, in the sense that their total variation distance vanishes exponentially. This result underpins key results in channel coding, wiretap secrecy, common randomness generation, and random-binning arguments. Despite its importance, the classical soft covering results address only the regime $R > I(X;Y)$. The regime $R < I(X;Y)$ — where the codebook rate is below the mutual information — has received comparatively little attention, and it turns out that it is considerably the more challenging and structurally richer regime.

In this paper, we study the soft covering phenomenon across *all* rates $R \geq 0$ by formulating it as a Neyman–Pearson hypothesis testing problem: Given an observed output sequence y^n, we ask: was it produced by the channel W driven by a randomly chosen codeword from $\mathcal{C}$ (hypothesis $\mathcal{H}_1$), or was it drawn independently from the marginal $P_Y^{\otimes n}$ (hypothesis $\mathcal{H}_0$)? The Neyman–Pearson test, based on the log-likelihood ratio (LLR) $\Lambda(y^n)$, decides in favor of $\mathcal{H}_1$ when $\Lambda(y^n) \geq \tau$, where τ is a threshold tuned to obtain a prescribed tolerable FA probability. The two error events are then: false alarm (FA): deciding in favor of $\mathcal{H}_1$ when $\mathcal{H}_0$ is true, and missed detection (MD): deciding in favor $\mathcal{H}_0$ when $\mathcal{H}_1$ is true. We derive the exact exponential decay rates $E_{\mathrm{FA}}(\tau, R)$ and $E_{\mathrm{MD}}(\tau, R)$ of the jointly averaged FA and MD error probabilities $\alpha_n(\tau, R)$ and $\beta_n(\tau, R)$, to be defined formally in Section 2.

The analysis reveals a considerably surprising phase structure in the (τ, R) plane, governed by two critical thresholds: $\tau = 0$ and $\tau^* = \max\{0, I(X;Y) - R\}$. For $\tau < 0$, the FA exponent vanishes (unless the channel has some singularity like the Z-channel) and the MD exponent is positive and channel-specific (see Remark 1). At $\tau = 0$, the picture depends critically on R. The FA exponent is always zero at $\tau = 0$ (with the above digression for singular channels), for every $R > 0$. The MD exponent at $\tau = 0$ undergoes a phase transition at $R = I(X;Y)$: it is strictly positive for $R < I(X;Y)$, and vanishes for $R \geq I(X;Y)$. The case $R = I(X;Y)$, $\tau = 0$, where *both* exponents simultaneously vanish, is the Neyman–Pearson exponent formulation of the soft covering phenomenon: at exactly the soft covering rate, neither error decays exponentially at threshold $\tau = 0$. For $\tau > 0$, both error exponents can be positive, and the picture depends on R. For $R < I(X;Y)$, there is a genuine tradeoff interval $\tau \in (0,\, I(X;Y) - R)$ where both error exponents are simultaneously positive. Beyond this interval (for $\tau \geq I(X;Y) - R$), the MD exponent drops to zero. The tradeoff interval has width $I(X;Y) - R$, which shrinks to zero as $R \nearrow I(X;Y)$. For $R \geq I(X;Y)$ at least one of the two exponents is zero no matter what the value of τ may be, in other words, there is no interval where both exponents are simultaneously positive. Specifically: for $\tau \leq 0$, the FA exponent is zero (FA probability does not decay exponentially); for $\tau \geq 0$, the MD exponent is zero (the codeword output is statistically easy to detect). The FA exponent is strictly positive for $\tau > 0$ and grows with τ, but over that same range the MD exponent is identically zero. The two zero-regions cover the entire real line, overlapping only at $\tau = 0$ where both exponents vanish simultaneously.

A structural asymmetry between the two exponents emerges from the formulas (stated precisely in Theorem 1). The FA exponent penalizes both the deviation of the channel output empirical distribution from the i.i.d. marginal, and the rate surplus of a codeword's mutual information over R, reflecting the rarity of the event that a noise sequence looks like a codeword output. The MD exponent penalizes only the deviation of the empirical channel from the true channel W, with no explicit rate term, reflecting the rarity of the event that a codeword output goes undetected. The proofs are based on large deviations properties concerning type-class enumerators [2, Chapter 4]. These enumerators are binomial random variables with exponentially many trials and exponentially decaying probabilities of

success.

A few words on earlier related work are in order.

Han and Verdú [1] introduced channel resolvability and established that the minimum rate R for which the mixture distribution $P_{Y^n|\mathcal{C}}$ can approximate $P_Y^{\otimes n}$ (in total variation or normalized KL divergence) equals $I(X;Y)$; this is the first-order result that forms the foundation of all subsequent work. The soft-covering lemma first appeared as Theorem 6.3 of Wyner [3], where it serves as a technical tool for the achievability proof of the common information theorem; it was later recognized as a central technique in wiretap secrecy, identification coding, and channel synthesis, and made the subject of systematic study by Han and Verdú [1] under the name of channel resolvability. A substantial body of later work derives the exact *exponential* rate of convergence of $P_{Y^n|\mathcal{C}}$ to $P_Y^{\otimes n}$ for $R > I(X;Y)$, under various distance measures. Hayashi [4] obtained a lower bound to the exponent under KL divergence. Parizi *et al.* [5] derived the exact exponent of th KL divergence with application to the wiretap channel. Yu and Tan [6] characterized the exact exponent under Rényi divergence of order $\alpha \in [0, 2]$ (which includes the Kullback-Leibler (KL) divergence as the limiting case $\alpha \to 1$) for i.i.d. random codes. Yagli and Cuff [7] established the exact exponent under total variation distance. Recently, Li *et al.* [8] derived a strong-converse exponent under the KL divergence. One a somewhat different research route, Cuff [9, 10] moved beyond the expected-value analysis to show that soft covering holds with probability doubly exponentially close to unity over the random codebook, enabling applications via the union bound. Cuff [11] also developed the theory of distributed channel synthesis, which relies on and strengthens the soft-covering lemma.

As mentioned above, Yu and Tan [6] characterized the exact exponential decay of the Rényi divergence of order $\alpha \in (0, 2)$ and $R > I(X;Y)$. There is a precise connection to hypothesis testing: the Rényi divergence of order α evaluated at the optimal $\alpha \in (0, 1)$ corresponds to the *Chernoff exponent* (symmetric Bayesian error exponent) of testing $P_Y^{\otimes n}$ against $P_{Y^n|\mathcal{C}}$. In Neyman–Pearson terms, this is the exponent achieved at the *specific threshold* τ that equalizes $E_{\text{FA}}(\tau, R)$ and $E_{\text{MD}}(\tau, R)$ (the Chernoff point); it does not give the full Neyman–Pearson operating characteristics.

The most closely related prior work is [12], which considers a model where a transmitter either sends a codeword from a random fixed-composition codebook of rate R, or is silent, outputting the all-zero vector $\mathbf{0}$. The receiver must jointly detect whether transmission occurred and, if so, decode the message. The figures of merit are the FA probability (deciding transmission when silent), the MD probability (deciding silent when transmitting), and a decoding error probability. For a fixed composition random codebook, [12] derives the optimal detector/decoder in an extended Neyman–Pearson sense and characterizes the exact random coding exponents of all three error probabilities as functions of the rate R and two threshold parameters $\alpha, \beta \in \mathbb{R}$. The analysis in [12] is based on the type-class enumeration method, the same fundamental tool used here. The similarities with the present work are as follows. Both papers formulate the problem model as a Neyman–Pearson binary hypothesis

testing ($\mathcal{H}_0$: pure noise, $\mathcal{H}_1$: codeword output), both use random fixed-composition codebooks, and both derive exact random-coding exponents via type-class enumeration. However, at the same time, there are several differences. The first is that in [12], under $\mathcal{H}_0$ the transmitter output is a repetitive symbol 0 that designates silence (no transmission), so under the null hypothesis, the channel output y^n is a response to the all-zero input vector, unlike the present work where y^n is the channel response to an i.i.d. input source, P_X. The second difference is that the analysis in [12] is valid for all $R \geq 0$, but is most natural for $R > 0$ with a non-trivial decoding task. The regime $R < I(X;Y)$ is not highlighted, and the soft-covering threshold $R = I(X;Y)$ does not play a special role in [12] since the hypotheses are always different regardless of R. In the present work, $R = I(X;Y)$ is the central threshold: it is where both error exponents simultaneously vanish, characterizing the soft covering phenomenon in Neyman–Pearson terms. Third, in [12] there is also a characterization of the exponent of the decoding error probability, which has no analogue here. Finally, in [12] there is no phase transition analogous to the one at $\tau = 0$ in the present work. Here, the behavior of $E_{\mathrm{MD}}(\tau, R)$ for $\tau \leq 0$ is a distinctive feature of the problem at hand.

The present paper differs from all prior work in the following respects.

1. *Full Neyman–Pearson tradeoff for all τ.* All prior exponent results for resolvability correspond to a fixed scalar distance measure (KL, total variation, Rényi), which is the expected distance averaged over both $\mathcal{C}$ and y^n. We instead characterize the complete Neyman–Pearson operating characteristic: the pair $(E_{\mathrm{FA}}(\tau, R), E_{\mathrm{MD}}(\tau, R))$ for every threshold τ, giving a full tradeoff curve rather than a single operating point.

2. *All rates $R \geq 0$.* Every previous exponent result for resolvability requires $R > I(X;Y)$. We handle all $R \geq 0$, including the unexplored regime $R < I(X;Y)$ where the codebook output is more concentrated than i.i.d. and where there is a genuine Neyman–Pearson tradeoff between FA and MD.

3. *Proof method and exactness.* Prior analyses apply Chernoff-type or Gallager-style bounding to the channel output distribution, which is a mixture of exponentially many conditional output distributions given the various input codewords. The Chernoff bound applied to a mixture of channel outputs is not automatically tight: prior papers establish tightness by a separate converse argument specific to each distance measure. In the present work, we avoid Chernoff bounds altogether. Instead, we apply the type-class enumeration method [2], which yields the *exact* exponential rate.

A statistical-physics perspective on soft covering across all rates, including connections to phase transitions, appears in [13].

The outline of the remaining part of this work is as follows. Section 2 establishes notation conventions and provides some background. Section 3 states the main theorem, whose proof appears in

the appendix 6. Section 4 develops the phase structure and the connection to soft covering. Section 5 illustrates the results on the Z-channel. Finally, in Section 6, we summarize the main findings and speculate on possible future research directions.

2 Notation Conventions and Basic Background

Let $\mathcal{X}$ and $\mathcal{Y}$ denote finite input and output alphabets. Sequences of length n are written in boldface-free lowercase, i.e., $x^n = (x_1, \ldots, x_n) \in \mathcal{X}^n$ and $y^n = (y_1, \ldots, y_n) \in \mathcal{Y}^n$, where $\mathcal{X}^n$ and $\mathcal{Y}^n$ are the n-th Cartesian powers of $\mathcal{X}$ and $\mathcal{Y}$, respectively. The *type* of a sequence $x^n \in \mathcal{X}^n$ is the empirical probability distribution $\hat{P}_{x^n}(a) = \frac{1}{n}\#\{i : x_i = a\}$, $a \in \mathcal{X}$. The equivalence set of all sequences in $\mathcal{X}^n$ of type P is called the *type class* $\mathcal{T}(P) \subseteq \mathcal{X}^n$. For a sequence pair $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$, the *joint type* Q_{XY} is the empirical distribution $Q_{XY}(a, b) = \frac{1}{n}\#\{i : x_i = a,\, y_i = b\}$, $a \in \mathcal{X}$, $b \in \mathcal{Y}$. Its marginals are denoted Q_X and Q_Y, and the conditional type $Q_{Y|X}$ is defined according to $Q_{XY}(a, b) = Q_X(a)Q_{Y|X}(b|a)$. We always restrict to joint types with $Q_X = P_X$, where P_X is some fixed input distribution. Throughout, $\hat{P}_{y^n}$ denotes the empirical distribution associated with y^n.

Information measures induced by a given probability distribution will be subscripted by the notation of this distribution. When this is an empirical distribution Q_{XY}, the subscript will be abbreviated by Q, in order to avoid cumbersome notation. Thus, $H_Q(Y) = -\sum_y Q_Y(y) \log Q_Y(y)$ is the marginal empirical entropy of an auxiliary random vector Y governed by Q_Y, $H_Q(Y|X) = -\sum_{x,y} Q_{XY}(x, y) \log Q_{Y|X}(y|x)$ is the conditional empirical entropy of Y given X, where (X, Y) are jointly governed by Q_{XY}, and $I_Q(X; Y) = H_Q(Y) - H_Q(Y|X)$ is the mutual information under Q_{XY}.

The discrete memoryless channel (DMC) with a finite input alphabet $\mathcal{X}$ and finite output alphabet $\mathcal{Y}$ will be denoted by $W : \mathcal{X} \to \mathcal{Y}$. When W is fed by an n-vector $x^n \in \mathcal{X}^n$, the corresponding channel output vector y^n is distributed according to

$$W^n(y^n|x^n) = \prod_{i=1}^{n} W(y_i|x_i). \tag{1}$$

The input distribution P_X is fixed throughout, with output marginal

$$P_Y(y) = \sum_x P_X(x)W(y|x) \tag{2}$$

and mutual information

$$I(X; Y) = \sum_{x,y} P_X(x)W(y|x) \log \frac{W(y|x)}{P_Y(y)}. \tag{3}$$

We also adopt the following shorthand notations.

$$D_{\mathrm{m}}(Q_Y) = D(Q_Y \| P_Y) = \sum_y Q_Y(y) \log \frac{Q_Y(y)}{P_Y(y)} \tag{4}$$

is the KL divergence between Q_Y and P_Y defined in (2). Also,

$$D_{\mathrm{c}}(Q_{XY}) = D(Q_{Y|X} \| W | P_X) = \sum_{x,y} P_X(x)Q_{Y|X}(y|x) \log \frac{Q_{Y|X}(y|x)}{W(y|x)} \tag{5}$$

is the conditional KL divergence between $Q_{Y|X}$ and the channel W with weighting P_X, and

$$\ell(Q_{XY}) = H_Q(Y|X) + D_{\mathrm{c}}(Q_{XY}) \tag{6}$$

is a notation used throughout in the proofs.

The data processing inequality (DPI) of the KL divergence implies that

$$D_{\mathrm{m}}(Q_Y) \le D_{\mathrm{c}}(Q_{XY}). \tag{7}$$

To see why this is true, observe that since $Q_X = P_X$,

$$\begin{aligned} D_{\mathrm{c}}(Q_{XY}) &= D(Q_{XY}\|P_X \otimes W) - D(Q_X\|P_X) \\ &= D(Q_{XY}\|P_X \otimes W) - D(P_X\|P_X) \\ &= D(Q_{XY}\|P_X \otimes W) \\ &\ge D(Q_Y\|P_Y) \\ &= D_{\mathrm{m}}(Q_Y), \end{aligned} \tag{8}$$

where the inequality is the DPI of the KL divergence applied to the marginalization map $(x, y) \mapsto y$.

For two positive sequences, $\{a_n\}_{n\ge1}$ and $\{b_n\}_{n\ge1}$, we write $a_n \doteq b_n$ to mean $\lim_{n\to\infty} \frac{1}{n} \log \frac{a_n}{b_n} = 0$. Accordingly, $a_n \doteq 0$ means that a_n decays faster than exponentially (e.g., doubly exponentially) and $a_n \doteq 1$ tells that a_n varies (grows or decays) at a sub-exponential rate, or even tends to a strictly positive constant. Throughout this paper, all logarithms are natural unless specified otherwise. We also denote the positive clipping operator by $[\cdot]_+$, which is defined by $[a]_+ = \max\{a, 0\}$ for any real a.

A random codebook $\mathcal{C} = \{x^n(m)\}_{m=1}^M$, $M = e^{nR}$, has codewords drawn independently at random under the uniform distribution across the type class $\mathcal{T}(P_X)$. Once the codebook $\mathcal{C}$ has been randomly selected, the induced output mixture is given by

$$P_{Y^n|\mathcal{C}}(y^n) = \frac{1}{M} \sum_{m=1}^{M} W^n(y^n|x^n(m)). \tag{9}$$

We denote $P_Y^{\otimes n}(y^n) = \prod_{i=1}^n P_Y(y_i)$, where the single-letter output marginal P_Y is induced by P_X and W as in (2).

In this paper, we focus on the following Neyman–Pearson hypothesis testing problem: Under hypothesis $\mathcal{H}_0$, y^n is governed by $P_Y^{\otimes n}$, and under hypothesis $\mathcal{H}_1$, y^n is drawn by $P_{Y^n|\mathcal{C}}$. The log-likelihood ratio (LLR) statistic is defined as

$$\Lambda(y^n) = \frac{1}{n} \ln \frac{P_{Y^n|\mathcal{C}}(y^n)}{P_Y^{\otimes n}(y^n)}. \tag{10}$$

The likelihood ratio test (LRT) with threshold τ decides in favor of $\mathcal{H}_1$ if $\Lambda(y^n) \ge \tau$; otherwise, it accepts $\mathcal{H}_0$.

The two kinds of error probabilities associated with the LRT are as follows. The false-alarm (FA) probability is

$$\alpha_n(\tau, R) = \mathbb{E}_{\mathcal{C}} \left\{ \sum_{\{y^n:\ \Lambda(y^n) \geq \tau\}} P_Y^{\otimes n}(y^n) \right\}, \tag{11}$$

and the missed detection (MD) probability is

$$\beta_n(\tau, R) = \mathbb{E}_{\mathcal{C}} \left\{ \sum_{\{y^n:\ \Lambda(y^n) < \tau\}} P_{Y^n|\mathcal{C}}(y^n) \right\}, \tag{12}$$

where in both (11) and (12), $\mathbb{E}_{\mathcal{C}}\{\cdot\}$ denotes expectation with respect to (w.r.t.) the randomness of the codebook $\mathcal{C}$. The corresponding error exponents are defined as

$$E_{\rm FA}(\tau, R) = -\lim_{n\to\infty} \frac{1}{n} \ln \alpha_n(\tau, R), \tag{13}$$

$$E_{\rm MD}(\tau, R) = -\lim_{n\to\infty} \frac{1}{n} \ln \beta_n(\tau, R), \tag{14}$$

where the existence of these limits will become apparent from the derivations to follow (Theorem 1).

The following quantity will be useful in the proofs. Given the randomly selected codebook, $\mathcal{C}$, and a channel output vector, y^n, the type-class enumerator (TCE) associated with type Q_{XY} and y^n is defined as

$$N(Q_{XY}|y^n) = \#\big\{m : (x^n(m), y^n) \in \mathcal{T}(Q_{XY})\big\}. \tag{15}$$

Clearly, the randomness of $\mathcal{C}$ induces randomness of $N(Q_{XY}|y^n)$. In particular, due to the independent random selection, $N(Q_{XY}|y^n)$ is a binomial random variable with $M = e^{nR}$ trials and success rate given by the probability that a single randomly chosen codeword from $\mathcal{T}(P_X)$ happens to have, together with y^n, the given joint type Q_{XY}. This probability is of the exponential order of $e^{-nI_Q(X;Y)}$. The unnormalized mixture under $\mathcal{H}_1$ can be easily expressed in terms of the TCE's as follows:

$$S(y^n) = \sum_{m=1}^{M} W^n(y^n|x^n(m)) = \sum_{Q_{XY}} N(Q_{XY}|y^n) e^{-n\ell(Q_{XY})}, \tag{16}$$

and so, $P_{Y^n|\mathcal{C}}(y^n) = S(y^n)/M$. For y^n of type $\hat{P}_{y^n} = Q_Y$, using $P_Y^{\otimes n}(y^n) = e^{-n[H_Q(Y) + D_{\rm m}(Q_Y)]}$:

$$\Lambda(y^n) = \frac{1}{n} \log S(y^n) - R + H_Q(Y) + D_{\rm m}(Q_Y). \tag{17}$$

To analyze the two kinds of probability of error, we shall invoke results concerning the large deviations behavior of $\{N(Q_{XY})\}$. Since these are binomial random variables, the following theorems from [2] (with a slight change in notation) will be useful.

(T1) **Theorem 4.1 of [2]**. For $N \sim \text{Binomial}(e^{nA}, e^{-nB})$ ($A > 0$ and $B > 0$) and $C \in \mathbb{R}$:

$$\lim_{n\to\infty} -\tfrac{1}{n} \ln \Pr\{N > e^{nC}\} = \begin{cases} [B - A]_+ & [A - B]_+ \geq C, \\ \infty & \text{elsewhere}, \end{cases} \tag{18}$$

$$\lim_{n\to\infty} -\tfrac{1}{n} \ln \Pr\{N < e^{nC}\} = \begin{cases} 0 & A - B < C, \\ \infty & A - B > C. \end{cases} \tag{19}$$

When $A > B$, $\Pr\{N > e^{nC}\} \doteq 1$ for $C \le A - B$, and $\Pr\{N < e^{nC}\}$ is doubly exponentially small for $C < A - B$. When $A < B$ and $C < 0$, $\Pr\{N > e^{nC}\} \doteq e^{-n(B-A)}$. We note in passing that the case $A = B$ is the case of asymptotic Poissonianity. In particular, if $N \sim \text{Binomial}(e^{nA}, \mu e^{-nA})$, then as $n \to \infty$, the distribution of N tends to a Poissonian random variable with parameter μ, i.e., $\Pr\{N = k\} \to \frac{\mu^k e^{-\mu}}{k!}$, $k = 0, 1, 2, \ldots$.

(T2) **Theorem 4.3 of [2]**. Let $N_j \sim \text{Binomial}(e^{nA_j}, e^{-nB_j})$, $j = 1, \ldots, k_n$, with $k_n \doteq 1$. Then for any thresholds $C_j \in \mathbb{R}$:

$$\Pr\Big\{\bigcap_j \{N_j \le e^{nC_j}\}\Big\} \doteq \mathbf{1}\Big\{\min_j (B_j - A_j + [C_j]_+) > 0\Big\}. \tag{20}$$

When $\min_j(B_j - A_j + [C_j]_+) > 0$, every $\Pr\{N_j > e^{nC_j}\}$ is either exponentially or doubly exponentially small (by Theorem 4.1 of [2]), and so, the union bound on the complementary events yields an intersection probability tending to 1. On the other hand, when $\min_j(B_j - A_j + [C_j]_+) \le 0$, then at least for some j, $B_j - A_j + [C_j]_+ \le 0$, and for that j, $\Pr\{N_j \le e^{nC_j}\} \doteq 0$, which implies that the intersection probability is a-fortiori $\doteq 0$. Note that there are no assumptions on the statistical dependence or independence among $\{N_j\}$.

It should be noted that in [2, Theorem 4.3], the assertion is formulated with a common threshold parameter C, rather than various thresholds C_j, as stated here. Nevertheless, the proof in [2] extends straightforwardly to allow different thresholds.

In view of those results, it is apparent that given y^n, a type Q_{XY} with $I_Q(X;Y) < R$ is a type that is typically populated with exponentially many codewords, in particular, $N(Q_{XY}|y^n)$ concentrates at the exponential order of $e^{n[R - I_Q(X;Y)]}$. Such a type will be henceforth referred to as a *bulk type*. By contrast, a type for which $I_Q(X;Y) > R$, is rarely populated, as the probability of for $N(Q_{XY}|y^n) \ge 1$ is of the exponential order of $e^{-n[I_Q(X;Y) - R]} \to 0$. Such a type will be referred to as a *sparse type*.

3 Main Result

For a joint type $Q = Q_{XY}$ with $Q_X = P_X$ and rate $R \ge 0$, let us define

$$\lambda(Q_{XY}, R) = D_{\text{m}}(Q_Y) - D_{\text{c}}(Q_{XY}) + [I_Q(X;Y) - R]_+. \tag{21}$$

By the DPI (7), $D_{\text{m}}(Q_Y) \le D_{\text{c}}(Q_{XY})$. Hence for bulk types ($I_Q(X;Y) \le R$): $\lambda(Q_{XY}, R) = D_{\text{m}}(Q_Y) - D_{\text{c}}(Q_{XY}) \le 0$. For the true channel $Q_{Y|X} = W$, $D_{\text{c}}(P_X \otimes W) = D(W\|W|P_X) = 0$ and $D_{\text{m}}(Q_Y) = D(P_Y\|P_Y) = 0$, and so, $\lambda(P_X \otimes W, R) = [I(X;Y) - R]_+$, which is positive for $R < I(X;Y)$, and zero for $R \ge I(X;Y)$.

Our main theorem, whose proof appears in the appendix, is the following.

Theorem 1. *For all $R \ge 0$ and $\tau \in \mathbb{R}$:*

$$E_{FA}(\tau, R) = \min_{\substack{Q:\ Q_X = P_X \\ \lambda(Q_{XY}, R) \ge \tau}} \big\{D_m(Q_Y) + [I_Q(X;Y) - R]_+\big\}. \tag{22}$$

For $R > 0$ and $\tau \in \mathbb{R}$:

$$E_{MD}(\tau, R) = \min_{\substack{Q_{XY}: Q_X = P_X \\ \lambda(Q_{XY}, R) < \tau \\ \Delta(Q_Y, R) < \tau}} D_c(Q_{XY}), \tag{23}$$

where

$$\Delta(Q_Y, R) = \max_{\substack{Q'_{XY}: Q'_X = P_X, Q'_Y = Q_Y \\ I_{Q'}(X;Y) \le R}} \big[D_m(Q_Y) - D_c(Q'_{XY})\big]. \tag{24}$$

For $\tau > 0$, the constraint $\Delta(Q_Y, R) < \tau$ is redundant (due to the DPI (7)) and the remaining active constraints are $Q_X = P_X$ and $\lambda(Q_{XY}, R) < \tau$.

Two remarks concerning this theorem are in order.

Remark 1. *For $\tau < 0$, missed detection requires the transmitted codeword to have a rare joint type, which is an unlikely event whose probability decays exponentially according to $D_c(Q_{XY})$. Given such an atypical transmitted pair, the interfering codewords are too weak to push the likelihood ratio above the (negative) threshold, and so, missed detection occurs with probability $\doteq 1$ conditional on this rare type. Hence $E_{MD}(\tau, R)$ is finite and positive for $\tau < 0$ (when $R < I(X;Y)$), governed by the same formula (23) as for $\tau > 0$. As $\tau \to -\infty$: the feasible set eventually empties and $E_{MD}(\tau, R) \to +\infty$.*

Remark 2 ($R = 0$: one codeword)**.** *For $R = 0$ ($M = 1$), the problem reduces to simple hypothesis testing of $W^n(\cdot|x^n(1))$ vs. $P_Y^{\otimes n}$ averaged over $x^n(1) \sim \text{Uniform}(\mathcal{T}(P_X))$. With a single codeword, $S(y^n) = e^{-n\ell(Q_{XY})}$ is deterministic, and both formulas (22)–(23) hold with $R = 0$ (the Δ constraint is vacuous since there are no interfering codewords). In particular, $E_{MD}(\tau, 0)$ is finite for all $\tau \in \mathbb{R}$ with no discontinuity, in contrast to $R > 0$.*

4 Properties and Phase Structure

We begin with an elementary observation that follows directly from Theorem 1.

Corollary 1 (Soft covering)**.** *For all $R \ge I(X;Y)$: $E_{FA}(0, R) = E_{MD}(0, R) = 0$.*

To see why this is true, observe that the type $Q_{XY} = P_X \otimes W$ has $D_{\mathrm{m}}(Q_Y) = 0$, $I_Q(X;Y) = I(X;Y) \le R$, $D_{\mathrm{c}}(Q_{XY}) = 0$, and $\lambda(Q_{XY}, R) = 0$, so it is feasible for $\tau = 0$ with zero cost, hence $E_{\mathrm{FA}}(0, R) = 0$. Likewise, $E_{\mathrm{MD}}(0, R) = 0$ since types arbitrarily close to $P_X \otimes W$ with $\lambda(Q_{XY}, R) < 0$ and $D_{\mathrm{c}}(Q_{XY}) \to 0$ exist by continuity.

This is the Neyman–Pearson implication of the soft covering lemma [1]: at $\tau = 0$, both error exponents simultaneously vanish when $R \ge I(X;Y)$, meaning the two hypotheses are exponentially indistinguishable. In other words, even if the FA and MD probabilities decay as $n \to \infty$, in this case, the rates of their decay are definitely slower than exponential.

4.1 Phase transitions

Both exponents have several regions of behavior as functions of τ. The following two propositions describe them.

Proposition 1 (FA: flat and active regions)**.** *Let Q^*_{XY} minimize $D_m(Q_Y) + [I_Q(X;Y) - R]_+$ over all Q_{XY} with $Q_X = P_X$, and define*

$$\tau_{\text{flat}}(R) := \lambda(Q^*_{XY}, R), \qquad \lambda_{\max}(R) := \max_{Q_{XY}: Q_X = P_X} \lambda(Q_{XY}, R). \tag{25}$$

$E_{FA}(\tau, R)$ has three regions:

(i) Flat: $\tau \le \tau_{\text{flat}}(R)$*: $E_{FA}(\tau, R) = D_m(Q^*_{XY}) + [I_{Q^*}(X;Y) - R]_+$ (constant in τ).*

(ii) Active: $\tau \in (\tau_{\text{flat}}(R), \lambda_{\max}(R))$*: $E_{FA}(\tau, R)$ strictly increases in τ.*

(iii) Infinite: $\tau > \lambda_{\max}(R)$*: $E_{FA}(\tau, R) = +\infty$.*

Proof. (i) For $\tau \le \tau_{\text{flat}}(R) = \lambda(Q^*_{XY}, R)$, the unconstrained minimizer Q^*_{XY} satisfies $\lambda(Q^*_{XY}, R) \ge \tau$ and hence is feasible. Since it achieves the global minimum, the constrained minimum equals the unconstrained one; $E_{\text{FA}}(\tau, R)$ is flat. (ii) For $\tau > \tau_{\text{flat}}(R)$, Q^*_{XY} is infeasible. The constrained minimum strictly exceeds the unconstrained one and strictly increases with τ as the feasible set shrinks. (iii) For $\tau > \lambda_{\max}(R)$, every type has $\lambda(Q_{XY}, R) \le \lambda_{\max}(R) < \tau$, so the feasible set is empty and $E_{\text{FA}}(\tau, R) = +\infty$ by convention. □

Proposition 2 (MD: zero, active, and divergent regions)**.** *Let $\tau^*(R) = [I(X;Y) - R]_+$ and $\lambda_{\min}(R) = \min_{Q_{XY}: Q_X = P_X} \lambda(Q_{XY}, R)$. For $R > 0$, $E_{MD}(\tau, R)$ has three regions:*

(i) Zero: $\tau \ge \tau^*(R)$*: $E_{MD}(\tau, R) = 0$.*

(ii) Active: $\tau \in (\lambda_{\min}(R), \tau^*(R))$*: $E_{MD}(\tau, R)$ is finite, positive, and strictly decreasing in τ.*

(iii) Infinite: $\tau \le \lambda_{\min}(R)$*: $E_{MD}(\tau, R) = +\infty$ (the feasible set $\{\lambda(Q_{XY}, R) < \tau\}$ is empty).*

Within the active region, there is a kink at some $\tau_{\text{kink}}(R) \in (\lambda_{\min}(R), 0)$ where the minimizing type transitions from bulk ($I_{Q^*}(X;Y) \le R$, for $\tau < \tau_{\text{kink}}$) to sparse ($I_{Q^*}(X;Y) > R$, for $\tau > \tau_{\text{kink}}$).

Proof. (i) For $\tau \ge \tau^*(R)$, types near $P_X \otimes W$ (with $D_{\text{c}}(Q_{XY}) \to 0$ and $\lambda(Q_{XY}, R) \to \tau^*(R)^-$) are feasible, giving $\inf D_{\text{c}}(Q_{XY}) = 0$ and $E_{\text{MD}}(\tau, R) = 0$. ii) Monotonicity in τ is immediate: the feasible set $\{\lambda(Q_{XY}, R) < \tau\}$ grows as τ increases, so $E_{\text{MD}}(\tau, R)$ is non-increasing. Strict decrease and positivity follow from the formula (23). (iii) For $\tau \le \lambda_{\min}(R)$, every type has $\lambda(Q_{XY}, R) \ge \lambda_{\min}(R) \ge \tau$, so the feasible set is empty and $E_{\text{MD}}(\tau, R) = +\infty$. □

4.2 The Neyman–Pearson tradeoff zone

The results above combine into a clean picture of the Neyman–Pearson tradeoff (Corollary 2 and Proposition 2).

Corollary 2. *Let* $\tau^*(R) := [I(X;Y) - R]_+$.

(i) For $R < I(X;Y)$*:* $E_{MD}(\tau, R) > 0$ *for all* $\tau < \tau^*(R)$*, and* $E_{MD}(\tau, R) = 0$ *for all* $\tau \geq \tau^*(R)$*. Both* $E_{FA}(\tau, R) > 0$ *and* $E_{MD}(\tau, R) > 0$ *simultaneously for all* $\tau \in (0, \tau^*(R))$*.*

(ii) For $R \geq I(X;Y)$*:* $\tau^*(R) = 0$*, so* $E_{MD}(\tau, R) = 0$ *for all* $\tau \geq 0$ *and* $E_{FA}(\tau, R) = 0$ *for all* $\tau \leq 0$*. Both exponents simultaneously vanish at* $\tau = 0$ *(Corollary 1), and the Neyman–Pearson tradeoff zone is empty.*

Proof. $E_{MD}(\tau, R) = 0$ *iff* $\tau \geq \tau^*(R)$. The only type with $D_c(Q_{XY}) = 0$ is $Q_{XY} = P_X \otimes W$, which has $\lambda(P_X \otimes W, R) = \tau^*(R)$. For $\tau \geq \tau^*(R)$, types approaching $P_X \otimes W$ have $D_c(Q_{XY}) \to 0$ and $\lambda \to \tau^*(R)^- < \tau$, so they are feasible with $D_c(Q_{XY}) \to 0$, giving $E_{\mathrm{MD}}(\tau, R) = 0$. For $\tau < \tau^*(R)$, every type with small $D_c(Q_{XY})$ has $Q_{Y|X}$ close to W and hence $\lambda(Q_{XY}, R)$ close to $\tau^*(R) > \tau$, so it is not feasible; thus $\inf_{\lambda(Q_{XY},R)<\tau} D_c(Q_{XY}) > 0$ and $E_{\mathrm{MD}}(\tau, R) > 0$.

$E_{FA}(\tau, R) > 0$ *for all* $\tau > 0$. A zero-cost type for $E_{\mathrm{FA}}(\tau, R)$ requires $Q_Y = P_Y$ and $I_Q(X;Y) \leq R$. Any such type has $\lambda(Q_{XY}, R) = -D_c(Q_{XY}) \leq 0$, so it is feasible for $E_{\mathrm{FA}}(\tau, R)$ (i.e. $\lambda(Q_{XY}, R) \geq \tau$) only if $\tau \leq 0$. Hence for $\tau > 0$ no zero-cost type is feasible and $E_{\mathrm{FA}}(\tau, R) > 0$.

Conclusion. For $R < I(X;Y)$: both $E_{\mathrm{FA}}(\tau, R) > 0$ (since $\tau > 0$) and $E_{\mathrm{MD}}(\tau, R) > 0$ (since $\tau < \tau^*(R)$) hold simultaneously iff $\tau \in (0, \tau^*(R))$. For $R \geq I(X;Y)$: $\tau^*(R) = 0$, so $E_{\mathrm{MD}}(\tau, R) = 0$ for all $\tau \geq 0$ and $E_{\mathrm{FA}}(\tau, R) = 0$ for all $\tau \leq 0$ (since $P_X \otimes W$ has $D_c(Q_{XY}) = 0$, $Q_Y = P_Y$, $I_Q(X;Y) = I(X;Y) \leq R$, giving a feasible zero-cost type for $E_{\mathrm{FA}}(\tau, R)$ whenever $\tau \leq 0$). Thus the two zero regions cover all of $\mathbb{R}$ and the tradeoff zone is empty. □

5 Numerical Illustration: Z-Channel

In the section, we demonstrate the behavior of both exponents for a numerical example of a Z-channel.

Let $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ and consider the Z-channel with the following input-output transition probabilities:

$$W(0|0) = 1, \tag{26}$$

$$W(1|0) = 0, \tag{27}$$

$$W(0|1) = w, \quad \text{and} \tag{28}$$

$$W(1|1) = 1 - w, \tag{29}$$

with $w = 0.45$ and $P_X(0) = P_X(1) = 0.5$. The corresponding mutual information is $I(X;Y) = 0.2441$ nats per channel use. Joint types are parameterized by $q = Q(0|1) \in (0, 1)$, with $Q(y|0) = W(y|0)$ forced. Defining the binary entropy function and the binary KL divergence as

$$h_{\mathrm{b}}(u) = -u \ln u - (1-u) \ln(1-u) \tag{30}$$

$$D_{\mathrm{b}}(u\|v)) = u \ln \frac{u}{v} + (1-u) \ln \frac{1-u}{1-v}, \tag{31}$$

where $(u, v) \in [0, 1]^2$, this gives

$$I_Q(X;Y) = h_{\mathrm{b}}\left(\tfrac{1+q}{2}\right) - \tfrac{1}{2}h_{\mathrm{b}}(q), \tag{32}$$

$$D_{\mathrm{c}}(Q_{XY}) = \tfrac{1}{2}D_{\mathrm{b}}(q\|w), \quad \text{and} \tag{33}$$

$$D_{\mathrm{m}}(Q_Y) = D_{\mathrm{b}}\left(\tfrac{1+q}{2}\middle\|\tfrac{1+w}{2}\right). \tag{34}$$

Seven figures follow, one per page, and each one contains a brief description and discussion, in addition to the figure caption.

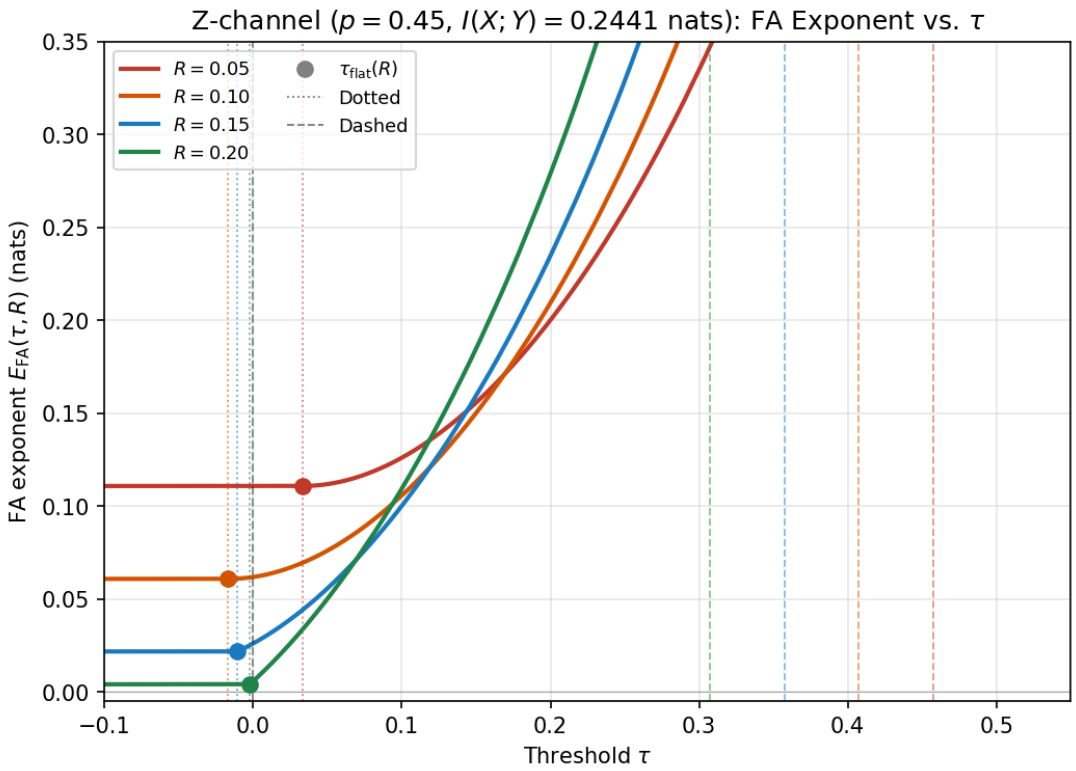

Figure 1: **FA exponent** $E_{\mathbf{FA}}(\tau, R)$ vs. τ for four rates.

In Fig. 1, for each rate $R \in \{0.05, 0.10, 0.15, 0.20\}$ (all below $I(X;Y) = 0.2441$), $E_{\text{FA}}(\tau, R)$ is flat at $E_{\text{FA,flat}}(R) = D_{\text{m}}(Q^*) + [I_{Q^*}(X;Y) - R]_+ > 0$ for $\tau \leq \tau_{\text{flat}}(R)$ (filled dots, dotted verticals), then strictly increases for $\tau > \tau_{\text{flat}}(R)$, diverging to $+\infty$ at $\lambda_{\max}(R)$ (dashed verticals). $E_{\text{FA}}(\tau, R)$ is continuous throughout. The flat value $E_{\text{FA,flat}}(R) > 0$ (rather than 0) is unique to singular channels like the Z-channel with $W(1|0) = 0$: a typical output y^n (which has many 1's) can only be explained by codewords that have '1' at every position where y^n has '1', and with only e^{nR} codewords drawn i.i.d. from P_X, the probability that even a single such compatible codeword exists is exponentially small. Hence $P_{Y^n|\mathcal{C}}(y^n) = 0$ with high probability over the ensemble of codes, $\Lambda(y^n) = -\infty$, and FA is exponentially rare for *any* finite τ, even $\tau \to -\infty$. See Figure 2 for a zoom on the active region.

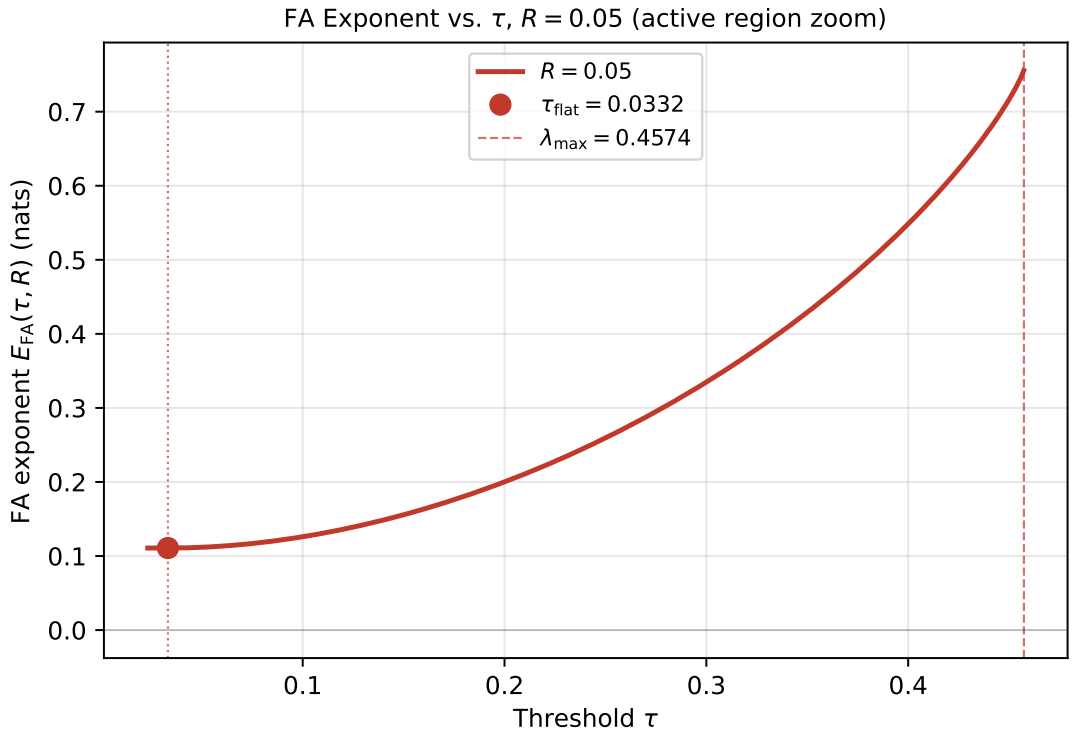

Figure 2: **Zoom into the active region of $E_{\mathbf{FA}}(\tau, R)$.** Normalized axes: $x = 0$ at $\tau_{\text{flat}}(R)$, $x = 1$ at $\lambda_{\max}(R)$. Only $R = 0.05$ (width ≈ 0.032 nats) is visible.

Fig. 2 provides a zoom into the active region $\tau \in (\tau_{\text{flat}}(R), \lambda_{\max}(R))$ for $R = 0.05$. At $\tau_{\text{flat}}(R) \approx 0.033$ (filled dot): $E_{\text{FA}}(\tau, R)$ lifts off its flat value ≈ 0.111 and begins to increase. At $\lambda_{\max}(R) \approx 0.457$ (dashed vertical): $E_{\text{FA}}(\tau, R) \to +\infty$. $E_{\text{FA}}(\tau, R)$ is strictly convex and monotone increasing throughout the active region.

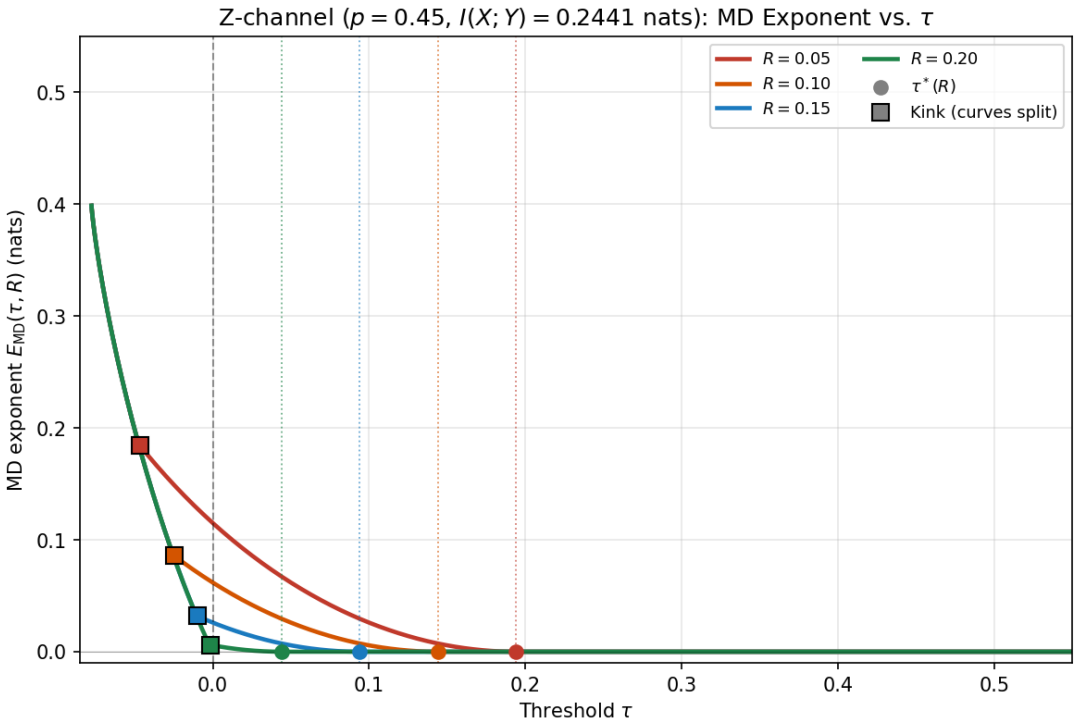

Figure 3: **MD exponent** $E_{\mathrm{MD}}(\tau, R)$ vs. τ for four rates $R \in \{0.05, 0.10, 0.15, 0.20\}$. Filled circles: $\tau^*(R) = [I(X;Y) - R]_+$ (onset of $E_{\mathrm{MD}}(\tau, R) = 0$).

In Fig. 3 we see the MD analogue of Fig. 1. $E_{\mathrm{MD}}(\tau, R)$ is monotone non-increasing in τ for each one of four rates as before. The curves start from $\tau \approx \lambda_{\min} \approx -0.078$ nats (minimum achievable $\lambda(Q_{XY}, R)$; $E_{\mathrm{MD}}(\tau, R) = +\infty$ for smaller τ).

Common branch. For τ sufficiently negative (below the leftmost kink at $\tau_{\mathrm{kink}}(R = 0.05) \approx -0.047$), all four curves are *exactly identical*: the minimizing type $Q^*(\tau)$ has $I_{Q^*}(X;Y) < R$ for all four rates, so the rate constraint is inactive and $\lambda(Q^*_{XY}, R) = D_{\mathrm{m}}(Q^*_Y) - D_{\mathrm{c}}(Q^*_{XY})$ is the same for all R.

Sequential splitting. As τ increases, the curves split one by one at the kink points $\tau_{\mathrm{kink}}(R)$ (filled squares), where $I_{Q^*}(X;Y) = R$ exactly and the minimizing type transitions from bulk to sparse. This is a first-order phase transition: the slope changes discontinuously, with the sparse branch (higher rate of decrease) taking over above the kink.

For $0 < \tau < \tau^*(R) = [I(X;Y) - R]_+$: $E_{\mathrm{MD}}(\tau, R) > 0$. At $\tau = \tau^*(R)$ (filled circles, dotted verticals): $E_{\mathrm{MD}}(\tau, R) = 0$.

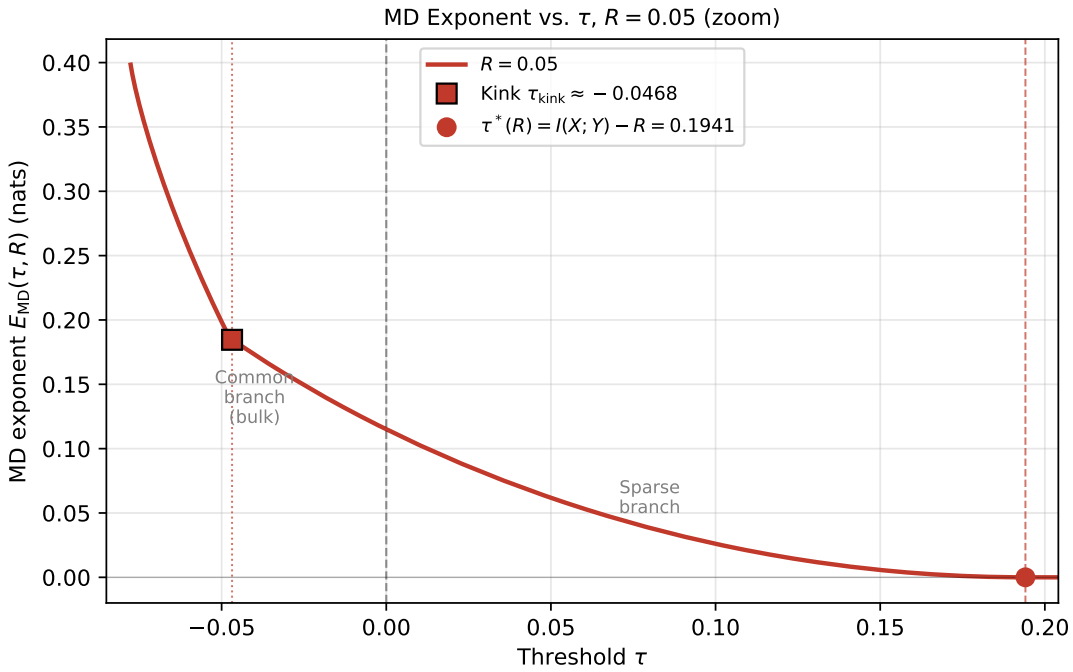

Figure 4: **Zoom into the active region of $E_{\text{MD}}(\tau, R)$, $R = 0.05$.** The kink at $\tau_{\text{kink}}(R) \approx -0.047$ (filled square, dotted vertical) marks the transition from the common bulk branch (left) to the sparse branch (right, rate-dependent). Filled circle: $\tau^*(R) = I(X;Y) - R \approx 0.194$ (onset of $E_{\text{MD}}(\tau, R) = 0$), dashed vertical.

Fig. 4 provides a zoom-in picture on $E_{\text{MD}}(\tau, R)$ for $R = 0.05$, revealing the full structure of the curve from $\lambda_{\min}(R)$ to $\tau^*(R)$. Left of the kink $\tau_{\text{kink}} \approx -0.047$: minimizing type is bulk, common to all rates. Right of the kink: minimizer becomes sparse, curves split by rate. $E_{\text{MD}}(\tau, R)$ is monotone non-increasing throughout, reaching zero at $\tau^*(R)$.

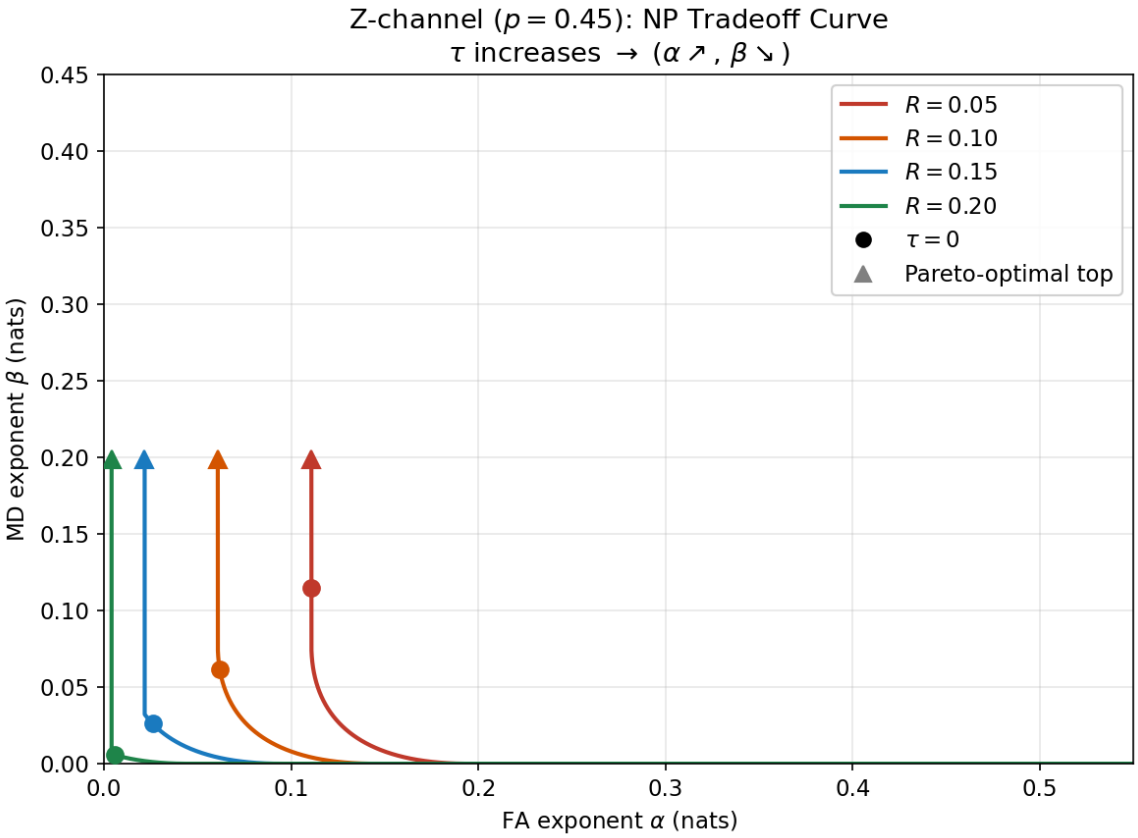

Figure 5: **Neyman–Pearson tradeoff curve**: $E_{\mathrm{MD}}(\tau, R)$ vs. $E_{\mathrm{FA}}(\tau, R)$, parametrized by τ (τ increasing: $E_{\mathrm{FA}}(\tau, R)$ ↗, $E_{\mathrm{MD}}(\tau, R)$ ↘). **Left**: raw parametric curve; vertical segments arise because $E_{\mathrm{FA}}(\tau, R)$ is flat while $E_{\mathrm{MD}}(\tau, R)$ decreases. Triangles: top of each vertical. **Right**: upper-envelope curve (each flat segment collapsed to its highest point).

Fig. 5 gives the parametric curve $(E_{\mathrm{FA}}(\tau, R), E_{\mathrm{MD}}(\tau, R))$ as τ sweeps the tradeoff range. It is shown for four rates. Each curve has a vertical segment where $E_{\mathrm{FA}}(\tau, R)$ is flat (Proposition 1) while $E_{\mathrm{MD}}(\tau, R)$ decreases: during this portion there is no genuine tradeoff, only a loss in MD performance at fixed $E_{\mathrm{FA}}(\tau, R)$. The right panel collapses each vertical segment to its highest point, revealing the genuine Neyman–Pearson tradeoff: to achieve larger $E_{\mathrm{FA}}(\tau, R)$ one must sacrifice $E_{\mathrm{MD}}(\tau, R)$.

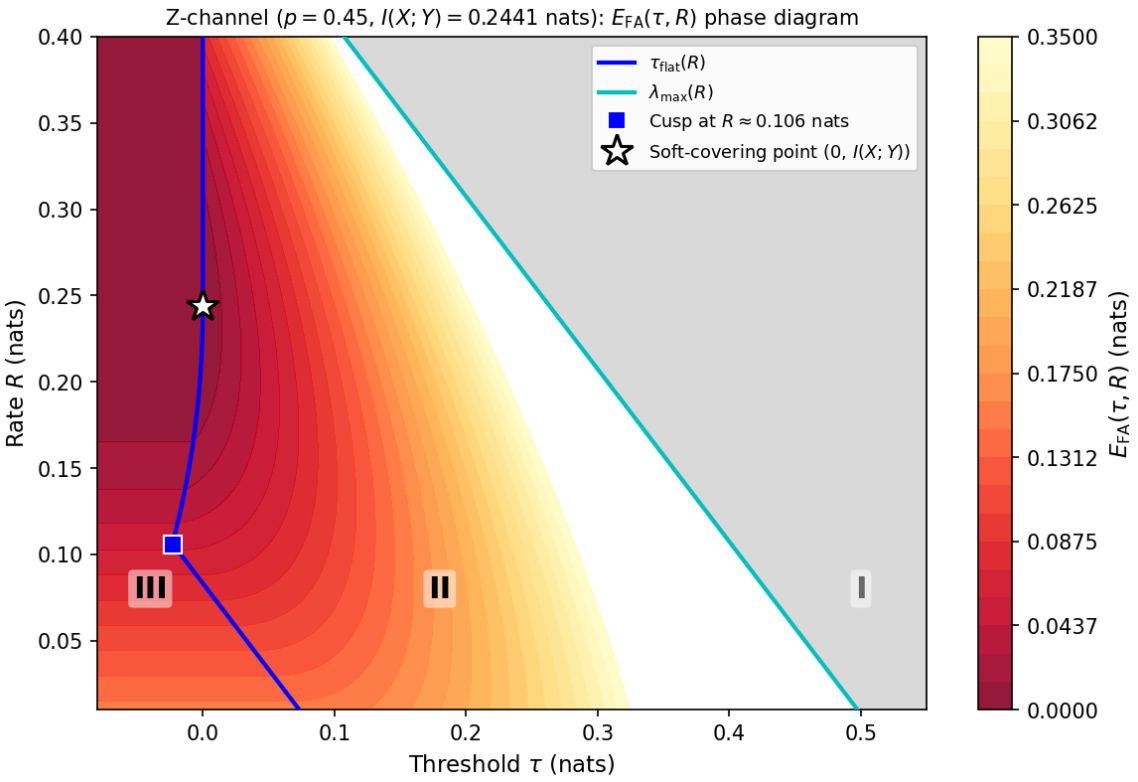

Figure 6: **FA exponent** $E_{\mathbf{FA}}(\tau, R)$: phase diagram in the (τ, R) plane (Proposition 1). Region **III** (left of blue curve, $\tau \leq \tau_{\mathrm{flat}}(R)$): E_{FA} is flat in τ (for fixed R) but varies with R. Region **II** (between blue and cyan curves, $\tau_{\mathrm{flat}}(R) < \tau < \lambda_{\max}(R)$): E_{FA} strictly increasing. Region **I** (grey, right of cyan curve, $\tau > \lambda_{\max}(R)$): $E_{\mathrm{FA}} = +\infty$. Blue curve: $\tau_{\mathrm{flat}}(R)$; cyan curve: $\lambda_{\max}(R)$. Blue square: cusp in $\tau_{\mathrm{flat}}(R)$ at $R \approx 0.106$ nats. White star: soft-covering point $(0, I(X;Y))$, at the boundary between Regions II and III.

Fig. 6 displays the three regions of Proposition 1 in the (τ, R) plane. Moving from left to right in τ: Region III (left of the blue curve $\tau_{\mathrm{flat}}(R)$, where E_{FA} is flat in τ for fixed R but varies with R) transitions into Region II (strictly increasing E_{FA}, between the blue and cyan curves), and finally into Region I ($E_{\mathrm{FA}} = +\infty$, grey, to the right of the cyan curve $\lambda_{\max}(R)$). The white star marks the soft-covering point $(\tau, R) = (0, I(X;Y))$; it lies at the boundary between Regions II and III (since $\tau_{\mathrm{flat}}(R) \to 0$ as $R \nearrow I(X;Y)$) and corresponds to $E_{\mathrm{FA}} = E_{\mathrm{FA,flat}}(R) > 0$, not zero. The blue square marks the cusp in $\tau_{\mathrm{flat}}(R)$ at $R = R_{\mathrm{cr}} \approx 0.106$ nats, where the unconstrained minimizer Q^*_{XY} transitions from a sparse type ($I_{Q^*} > R$, slope -1) to a bulk type, creating the visible kink in the blue curve.

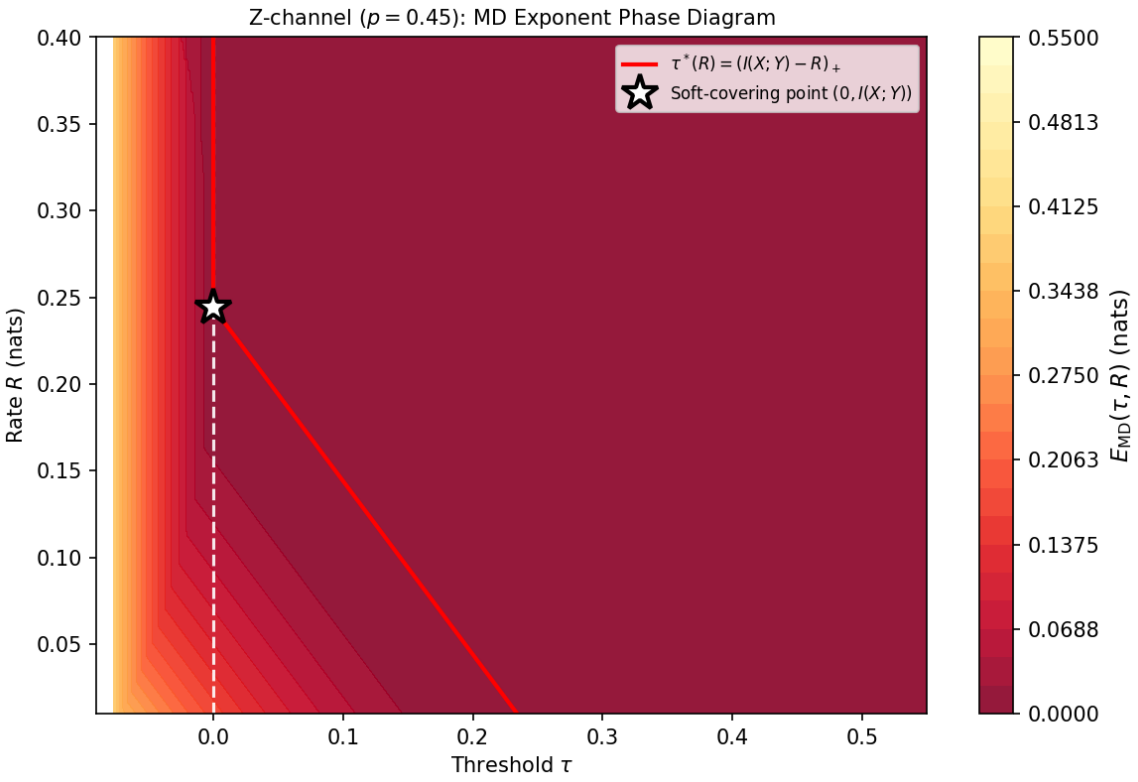

Figure 7: **MD exponent** $E_{\mathrm{MD}}(\tau, R)$: phase diagram. Shaded region ($\tau \leq 0$): $E_{\mathrm{MD}}(\tau, R)$ finite and positive when the feasible set $\{\lambda(Q_{XY}, R) < \tau\}$ is non-empty (Remark 1); $E_{\mathrm{MD}}(\tau, R) = +\infty$ otherwise. Colored region ($\tau > 0$): $E_{\mathrm{MD}}(\tau, R)$ finite, with sharp transition to 0 at $\tau^*(R) = [I(X;Y) - R]_+$ (red line). White dashed line: $\tau = 0$. White star: soft-covering point $(0, I(X;Y))$.

In Fig. 7 the shaded region ($\tau \leq 0$) has finite $E_{\mathrm{MD}}(\tau, R)$ given by $\min_{\lambda(Q_{XY},R)<\tau} D_{\mathrm{c}}(Q_{XY})$ when the feasible set is non-empty, and $E_{\mathrm{MD}}(\tau, R) = +\infty$ otherwise (Remark 1). The white dashed line at $\tau = 0$ marks $E_{\mathrm{MD}}(\tau, R) = 0$. The colored region ($\tau > 0$) shows finite $E_{\mathrm{MD}}(\tau, R)$, with a sharp transition to 0 at $\tau^*(R) = [I(X;Y) - R]_+$ (red line, slope -1). Together, the two phase diagrams show that the Neyman–Pearson tradeoff zone $0 < \tau < \tau^*(R)$ shrinks as $R \nearrow I(X;Y)$ and vanishes at $R = I(X;Y)$, the soft-covering threshold.

6 Conclusion and Outlook

We studied the soft covering lemma through the lens of Neyman–Pearson hypothesis testing, asking: can an observer distinguish the random codebook mixture $P_{Y^n|\mathcal{C}}$ from the i.i.d. distribution $P_Y^{\otimes n}$? We derived exact single-letter formulas for the FA and MD exponents $E_{\mathrm{FA}}(\tau, R)$ and $E_{\mathrm{MD}}(\tau, R)$ for all rates $R \geq 0$ and all thresholds $\tau \in \mathbb{R}$, using the type-class enumeration toolbox of [2]. The main findings are:

1. *Soft covering as a phase transition.* At $R = I(X;Y)$ and $\tau = 0$, both exponents simultaneously vanish — the Neyman–Pearson exponent characterization of the soft covering phenomenon. For $R < I(X;Y)$, a genuine Neyman–Pearson tradeoff interval $(0, I(X;Y) - R)$ exists where both exponents are positive. For $R \geq I(X;Y)$, the two zero regions cover all of $\mathbb{R}$, leaving no tradeoff

interval.

2. *Rich phase structure.* The FA exponent $E_{\mathrm{FA}}(\tau, R)$ is flat (constant in τ) below $\tau_{\mathrm{flat}}(R)$ and strictly increasing above it, diverging at $\lambda_{\max}(R)$. The MD exponent $E_{\mathrm{MD}}(\tau, R)$ is strictly decreasing in τ, with a kink at $\tau_{\mathrm{kink}}(R) < 0$ (a first-order phase transition where the minimizing type changes from bulk to sparse), and reaches zero at $\tau^*(R) = (I(X;Y) - R)_+$.
3. *Structural asymmetry.* The FA exponent penalizes both the empirical output deviation from P_Y and the rate surplus $[I_Q(X;Y) - R]_+$. The MD exponent penalizes only the channel divergence $D_{\mathrm{c}}(Q_{XY})$, with an additional constraint $\Delta(Q_Y, R) < \tau$ that identifies which transmitted types contribute — automatically satisfied for $\tau > 0$ by the DPI.

Several directions are open for future work.

1. *Beyond the annealed average.* The exponents derived here are for the annealed (codebook-averaged) probabilities $\mathbb{E}_{\mathcal{C}}[\alpha_n]$ and $\mathbb{E}_{\mathcal{C}}[\beta_n]$. The quenched (almost-sure or typical-codebook) exponents may differ and are generally harder to characterize. The regime $R < I(X;Y)$ may exhibit a gap between annealed and quenched exponents, as is common in disordered systems (see, e.g., [13]).
2. *Mismatched and compound channels.* The detector here is the optimal Neyman–Pearson test based on the true channel W. Characterizing the exponents under a mismatched detector (one that assumes a wrong channel $\tilde{W}$) would be natural, especially in the context of covert communications where the adversary may not know the exact codebook distribution.
3. *Finite-block-length refinements.* The exponent results give the leading exponential term. Sub-exponential (polynomial) pre-factors, as in [2], would sharpen the approximation and may reveal further phase transitions at the second order.
4. *Other channels and source models.* The analysis here is for discrete memoryless channels. Extensions to continuous alphabet channels (most notably, Gaussian), channels with memory, or multi-terminal settings (broadcast, multiple access) would broaden the scope and may uncover new structural phenomena.

Appendix – Proof of Theorem 1

6.1 The FA exponent

We prove (22) for $R > 0$; the case $R = 0$ follows by a direct type-counting argument (see Remark 2).

First, observe that

$$\alpha_n(\tau, R) = \sum_{y^n} P_Y^{\otimes n}(y^n) \cdot \Pr\left\{S(y^n) \geq e^{n\theta(y^n)} | y^n\right\}, \tag{A.1}$$

where conditional probabilities $\Pr\{\cdot|y^n\}$ are w.r.t. the randomness of $\mathcal{C}$ while y^n is fixed, and where,

using (17), the FA condition $\Lambda(y^n) \geq \tau$ is equivalent to $S(y^n) \geq e^{n\theta(y^n)}$ with

$$\theta(y^n) = \tau + R - H_Q(Y) - D_{\mathrm{m}}(Q_Y), \qquad Q_Y = \hat{P}_{y^n}. \tag{A.2}$$

Note that $\theta(y^n)$ depends on y^n only through its type $Q_Y = \hat{P}_{y^n}$. Now, fix y^n, let $\theta = \theta(y^n)$, and $Q_Y = \hat{P}_{y^n}$. Then,

$$\Pr\{S(y^n) \geq e^{n\theta} | y^n\} \doteq \Pr\left[\bigcup_{\substack{Q_{XY}:\ Q_X = P_X \\ Q_Y = \hat{P}_{y^n}}} \{N(Q_{XY}|y^n) \geq e^{n[\theta + \ell(Q_{XY})]}\} \middle| y^n \right], \tag{A.3}$$

where the union is over all types, Q_{XY}, with marginals $Q_X = P_X$ and $Q_Y = \hat{P}_{y^n}$. Since this is a union over a sub-exponential number of events, this probability is dominated by the largest probability term of the form $\Pr\{N(Q_{XY}|y^n) \geq e^{n[\theta+\ell(Q_{XY})]}\}$. We apply Theorem 4.1 of [2] (see (18)) to each $N(Q_{XY}|y^n) \sim \text{Binomial}(M, e^{-nI_Q(X;Y)})$, and the threshold exponent

$$\begin{aligned} \theta + \ell(Q_{XY}) &= \tau + R - H_Q(Y) - D_{\mathrm{m}}(Q_Y) + H_Q(Y|X) + D_{\mathrm{c}}(Q_{XY}) \\ &= \tau - (D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY})) + R - I_Q(X;Y). \end{aligned} \tag{A.4}$$

We next distinguish between bulk types ($I_Q(X;Y) \leq R$) and sparse types ($I_Q(X;Y) > R$). Beginning from bulk types, by (18), the upper-tail exponent is 0 when $R - I_Q(X;Y) \geq \theta + \ell(Q_{XY})$, and ∞ otherwise. On substituting (A.4), we obtain

$$R - I_Q(X;Y) \geq \tau - (D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY})) + R - I_Q(X;Y). \tag{A.5}$$

The terms R and $I_Q(X;Y)$ on both sides cancel, giving $D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY}) \geq \tau$. Since $I_Q(X;Y) \leq R$, definition (21) gives $\lambda(Q_{XY}, R) = D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY})$, and so, the condition is $\lambda(Q_{XY}, R) \geq \tau$. Therefore, for bulk types,

$$\Pr\{N(Q_{XY}|y^n) > e^{n[\theta+\ell(Q_{XY})]} | y^n\} \doteq \begin{cases} 1 & \lambda(Q_{XY}, R) \geq \tau, \\ 0 & \lambda(Q_{XY}, R) < \tau. \end{cases} \tag{A.6}$$

Moving on to sparse types, eq. (18) tells us that the upper-tail exponent is $I_Q(X;Y) - R$ when $[R - I_Q(X;Y)]_+ = 0 \geq \theta + \ell(Q_{XY})$, and ∞ otherwise. Substituting (A.4), the condition $\theta + \ell(Q_{XY}) \leq 0$ becomes:

$$\tau - (D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY})) + R - I_Q(X;Y) \leq 0, \tag{A.7}$$

i.e., $D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY}) + I_Q(X;Y) - R \geq \tau$. Since $I_Q(X;Y) > R$, definition (21) gives $\lambda(Q_{XY}, R) = D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY}) + I_Q(X;Y) - R$, so the condition is again $\lambda(Q_{XY}, R) \geq \tau$. Therefore, for sparse types,

$$\Pr\left\{N(Q_{XY}|y^n) > e^{n[\theta+\ell(Q_{XY})]} | y^n\right\} \doteq \begin{cases} e^{-n(I_Q(X;Y)-R)} & \lambda(Q_{XY}, R) \geq \tau, \\ 0 & \lambda(Q_{XY}, R) < \tau. \end{cases} \tag{A.8}$$

For each fixed marginal type Q_Y, we maximize over all conditional types $Q_{X|Y}$ with $Q_X = P_X$. The threshold $\theta = \tau + R - H_Q(Y) - D_{\mathrm{m}}(Q_Y)$ depends on y^n only through Q_Y (via $\hat{P}_{y^n}$), while $\ell(Q_{XY})$

and hence $\theta + \ell(Q_{XY})$ depend on the full joint type Q_{XY}. After maximizing over $Q_{X|Y}$, however, the dominant exponent depends on y^n only through Q_Y. We may therefore group the sum in (A.1) by types:

$$\alpha_n(\tau, R) \doteq \sum_{Q_Y} \underbrace{\sum_{y^n:\ \hat{P}_{y^n}=Q_Y} P_Y^{\otimes n}(y^n)}_{\doteq e^{-nD_{\mathrm{m}}(Q_Y)}} \cdot \max_{\substack{Q:\, Q_X=P_X \\ Q_Y \text{ fixed}}} \Pr\big\{N(Q_{XY}|y^n) \geq e^{n[\theta+\ell(Q_{XY})]}|y^n\big\}. \tag{A.9}$$

The dominant contribution to (A.9) comes from the type Q_{XY} minimizing the total exponent. Since both cases unify as $D_{\mathrm{m}}(Q_Y) + [I_Q(X;Y) - R]_+$ subject to $\lambda(Q_{XY}, R) \geq \tau$, this yields (22).

6.2 The MD exponent

Similarly as above, we prove (23) for $R > 0$, the case $R = 0$ follows by a direct argument (see Remark 2).

Owing to the symmetry of the random coding mechanism, we assume, without loss of generality that the transmitted codeword is $x^n(1)$. Under $\mathcal{H}_1$, the pair $(x^n(1), y^n)$ is drawn from $P_{X^n} \times W^n$. By the method of types:

$$\Pr\big\{(x^n(1), y^n) \in \mathcal{T}(Q_{XY})\big\} \doteq e^{-nD_{\mathrm{c}}(Q_{XY})} \tag{A.10}$$

for any joint type Q_{XY} with $Q_X = P_X$. We condition on this type and treat the remaining $M - 1$ codewords $x^n(m)$, $m = 2, 3, \ldots, M$ as random.

We next show that if $\lambda(Q_{XY}, R) \geq \tau$ then the MD event is virtually impossible. Given that $(x^n(1), y^n)$ has joint type Q_{XY} (so y^n has marginal type Q_Y), recall that $\theta = \tau + R - H_Q(Y) - D_{\mathrm{m}}(Q_Y)$ as in (A.2). Decompose

$$S(y^n) = e^{-n\ell(Q_{XY})} + \widetilde{S}(y^n), \tag{A.11}$$

where $e^{-n\ell(Q_{XY})} = W^n(y^n|x^n(1))$ is the deterministic contribution of the transmitted codeword and $\widetilde{S}(y^n) = \sum_{m=2}^{M} W^n(y^n|x^n(m))$ is the contribution of the remaining random codewords. The MD event is equivalent to $S(y^n) < e^{n\theta}$. Once again, we treat bulk types and sparse types separately.

Considering sparse types first, observe that since $S(y^n) \geq e^{-n\ell(Q_{XY})}$, it suffices to show $-\ell(Q_{XY}) \geq \theta$. Expanding using the definitions of $\ell(Q_{XY})$ and θ:

$$\begin{aligned}
-\ell(Q_{XY}) \geq \theta &\iff -H_Q(Y|X) - D_{\mathrm{c}}(Q_{XY}) \geq \tau + R - H_Q(Y) - D_{\mathrm{m}}(Q_Y) \\
&\iff D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY}) + I_Q(X;Y) - R \geq \tau \\
&\iff \lambda(Q_{XY}, R) \geq \tau,
\end{aligned}$$

where the last equivalence uses the relation $\lambda(Q_{XY}, R) = D_{\mathrm{m}}(Q_Y) - D_{\mathrm{c}}(Q_{XY}) + I_Q(X;Y) - R$, which holds for sparse types ($I_Q(X;Y) > R$). This holds by assumption, so $S(y^n) \geq e^{n\theta}$ deterministically given $(x^n(1), y^n)$, and so, the MD event is impossible.

Passing on to bulk types, to show that the MD event is virtually impossible when $\lambda(Q_{XY}, R) > \tau$, assume conversely that $\lambda(Q_{XY}, R) > \tau$ (handling the boundary $\lambda(Q_{XY}, R) = \tau$ by continuity at

the end). Consider the interfering codewords that share the *same* joint type Q_{XY} with y^n as the transmitted one, $x^n(1)$. Their contribution to $\widetilde{S}(y^n)$ gives

$$S(y^n) \geq \widetilde{S}(y^n) \geq \widetilde{N}(Q_{XY}|y^n) \cdot e^{-n\ell(Q_{XY})}, \tag{A.12}$$

where here $\widetilde{N}(Q_{XY}|y^n) \sim \text{Binomial}(M-1,\, e^{-nI_Q(X;Y)})$ with $M - 1 \doteq e^{nR}$. Expanding $\theta + \ell(Q_{XY})$ from the definitions, we have

$$\begin{aligned}\theta + \ell(Q_{XY}) &= (\tau + R - H_Q(Y) - D_{\text{m}}(Q_Y) + (H_Q(Y|X) + D_{\text{c}}(Q_{XY}) \\ &= \tau - \big(D_{\text{m}}(Q_Y) - D_{\text{c}}(Q_{XY})\big) + R - I_Q(X;Y). \end{aligned} \tag{A.13}$$

Since $D_{\text{m}}(Q_Y) - D_{\text{c}}(Q_{XY}) = \lambda(Q_{XY}, R) \geq \tau$ and $R - I_Q(X;Y) \geq 0$, we get $\theta + \ell(Q_{XY}) \leq R - I_Q(X;Y)$, with strict inequality when $\lambda(Q_{XY}, R) > \tau$. By Theorem 4.1 of [2] (19), $\Pr\{\widetilde{N}(Q_{XY}|y^n) < e^{n(\theta+\ell(Q_{XY}))}|x^n(1), y^n\}$ is doubly exponentially small whenever $\theta + \ell(Q_{XY}) < R - I_Q(X;Y)$, i.e. whenever $\lambda(Q_{XY}, R) > \tau$. Hence with probability $\doteq 1$,

$$S(y^n) \geq \widetilde{N}(Q_{XY}|y^n) \cdot e^{-n\ell(Q_{XY})} \geq e^{n[\theta+\ell(Q_{XY}])} \cdot e^{-n\ell(Q_{XY})} = e^{n\theta}, \tag{A.14}$$

so the MD event is virtually impossible in the sense that its probability decays doubly exponentially.

In both cases, $\lambda(Q_{XY}, R) \geq \tau$ implies $\Pr\{\text{MD}|x^n(1), y^n\} \doteq 0$. Hence only types Q_{XY} of $(x^n(1), y^n)$ with $\lambda(Q_{XY}, R) < \tau$ can contribute to the MD probability on the exponential scale. We next evaluate this contribution.

Now, fix a type Q_{XY} of $(x^n(1), y^n)$ with $\lambda(Q_{XY}, R) < \tau$. As mentioned earlier, the threshold $\theta = \tau + R - H_Q(Y) - D_{\text{m}}(Q_Y)$ depends on y^n only through its marginal Q_Y, and on τ, but not on any other property of Q_{XY}. For each possible joint type Q'_{XY} of an interfering codeword $x^n(m)$, $m = 2, 3, \ldots, M$, with y^n, the enumerator $\widetilde{N}(Q'_{XY}|y^n) \sim \text{Binomial}(M-1, e^{-nI_{Q'}(X;Y)})$. The event $\{\widetilde{S}(y^n) < e^{n\theta}\}$ is equivalent to the event that $\widetilde{N}(Q'_{XY}|y^n) \leq e^{n[\theta+\ell(Q'_{XY})]}$ for all Q'_{XY} simultaneously. To assess the probability of this intersection probability, we invoke Theorem 4.3 of [2] (see (20)). To this end, we compute $\theta + \ell(Q'_{XY})$ for each type Q'_{XY} of an interfering codeword. Since all interfering types Q'_{XY} share the marginal Q_Y of y^n, we have $D_{\text{m}}(Q'_Y) = D_{\text{m}}(Q_Y)$, and so,

$$\begin{aligned}\theta + \ell(Q'_{XY}) &= \tau + R - H_Q(Y) - D_{\text{m}}(Q_Y) + H_{Q'}(Y|X) + D_{\text{c}}(Q'_{XY}) \\ &= \tau - [D_{\text{m}}(Q'_Y) - D_{\text{c}}(Q'_{XY})] + R - I_{Q'}(X;Y). \end{aligned} \tag{A.15}$$

Note that this depends on Q'_{XY} of the interfering codewords, and on τ, but *not* on the type Q_{XY} of $(x^n(1), y^n)$ beyond its marginal Q_Y, which is already absorbed into $D_{\text{m}}(Q'_Y) = D_{\text{m}}(Q_Y)$. Upon applying Theorem 4.3 of [2], we obtain

$$\Pr\Big[\bigcap_{Q'_{XY}} \big\{\widetilde{N}(Q'_{XY}|y^n) \leq e^{n[\theta+\ell(Q'_{XY})]}\Big| x^n(1), y^n\big\}\Big] \doteq \mathbf{1}\Big\{\min_{Q'_{XY}}\big[I_{Q'}(X;Y) - R + [\theta + \ell(Q'_{XY})]_+\big] > 0\Big\}. \tag{A.16}$$

Let us define then

$$f(Q'_{XY}) = I_{Q'}(X;Y) - R + [\theta + \ell(Q'_{XY})]_+. \tag{A.17}$$

Using the simple identity, $a + [b-a]_+ \equiv \max\{a, b\}$ with $a = I_{Q'}(X;Y) - R$ and $b = \tau - [D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY})]$, and (A.15), we may rewrite the function f as

$$f(Q'_{XY}) = \max\big\{I_{Q'}(X;Y) - R, \tau - [D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY})]\big\}. \tag{A.18}$$

We next simplify $f(Q'_{XY})$. For sparse interfering types ($I_{Q'}(X;Y) > R$), $f(Q'_{XY}) \geq I_{Q'}(X;Y) - R > 0$ always. Hence sparse types never 'threaten' the occurrence of the event $\{\min_{Q'_{XY}} f(Q'_{XY}) > 0\}$ and can be excluded. For bulk interfering types, $I_{Q'}(X;Y) - R \leq 0$, and so, the occurrence of the event $\{\min_{Q'_{XY}} f(Q'_{XY}) > 0\}$ depends on the sign of $\tau - [D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY})]$. Thus the condition $\min_{Q'_{XY}} f(Q'_{XY}) > 0$ over all Q'_{XY} reduces to

$$\max_{\substack{Q'_{XY}:\, Q'_X = P_X,\, Q'_Y = Q_Y \\ I_{Q'}(X;Y) \leq R}} \big[D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY})\big] < \tau, \tag{A.19}$$

which is exactly the condition $\Delta(Q_Y, R) < \tau$ as defined in the theorem.

For $\tau > 0$, the DPI (7) gives $D_{\rm c}(Q'_{XY}) \geq D_{\rm m}(Q'_Y) = D_{\rm m}(Q_Y)$, and so, $D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY}) \leq 0 < \tau$, which means that the condition $\Delta(Q_Y, R) < \tau$ holds automatically for every Q_{XY}, and so, the corresponding constraint is slack. Thus $\Pr\{\widetilde{S}(y^n) < e^{n\theta}\} \doteq 1$ for every feasible transmitted type. On the other hand, for $\tau \leq 0$, $D_{\rm m}(Q_Y) - D_{\rm c}(Q'_{XY})$ may be larger than or equal to τ, making $\Delta(Q_Y, R) \geq \tau$ possible, in which case the indicator in (A.16) equals 0 and then $\Pr\{\widetilde{S}(y^n) < e^{n\theta} | x^n(1), y^n\} \doteq 0$.

The conclusion is that for $\tau > 0$, $\Pr\{\widetilde{S}(y^n) < e^{n\theta} | x^n(1), y^n\} \doteq 1$ for every transmitted type Q_{XY} with $\lambda(Q_{XY}, R) < \tau$. Together with $\Pr[\mathrm{MD}|Q_{XY}] \doteq 0$ when $\lambda(Q_{XY}, R) \geq \tau$), we have $\Pr\{\mathrm{MD} \mid Q_{XY} | x^n(1), y^n\} \doteq \mathbf{1}\{\lambda(Q_{XY}, R) < \tau\}$. Summing over all transmitted types:

$$\beta_n(\tau, R) \doteq \sum_{\substack{Q:\, Q_X = P_X \\ \lambda(Q_{XY}, R) < \tau}} e^{-nD_{\rm c}(Q_{XY})} \doteq \exp\Big\{-n \min_{\substack{Q:\, Q_X = P_X \\ \lambda(Q_{XY}, R) < \tau}} D_{\rm c}(Q_{XY})\Big\}, \tag{A.20}$$

giving $E_{\rm MD}(\tau, R) = \min_{\lambda(Q_{XY}, R) < \tau} D_{\rm c}(Q_{XY})$. However, for $\tau \leq 0$ a type Q_{XY} of $(x^n(1), y^n)$ with $\lambda(Q_{XY}, R) < \tau \leq 0$ contributes to β_n at the exponential scale provided that the additional condition, $\Delta(Q_Y, R) < \tau$, holds too. On the other hand, if $\Delta(Q_Y, R) < \tau$, Theorem 4.3 of [2] yields $\Pr\{\widetilde{S}(y^n) < e^{n\theta} | x^n(1), y^n\} \doteq 1$, and this type contributes $e^{-nD_{\rm c}(Q_{XY})}$ to β_n. If $\Delta(Q_Y, R) \geq \tau$, some bulk type of an interfering codeword Q'_{XY} gives $f(Q'_{XY}) \leq 0$, and Theorem 4.3 of [2] gives $\Pr\{\widetilde{S}(y^n) < e^{n\theta} | x^n(1), y^n\} \doteq 0$ (doubly exponentially small), and this type does not contribute at the exponential scale. Hence,

$$\beta_n(\tau, R) \doteq \sum_{\{Q_{Y|X}:\ \lambda(Q_{XY}, R) < \tau,\ \Delta(Q_Y, R) < \tau\}} e^{-nD_{\rm c}(Q_{XY})}, \tag{A.21}$$

giving (23). This establishes (23) in both cases.

References

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

[2] N. Merhav and N. Weinberger, "A Toolbox for Refined Information-Theoretic Analyses with Applications," *Foundations and Trends in Comm. and Inf. Theory*, vol. 22, no. 1, pp. 1–184, 2025.

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

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

[5] M. Bastani Parizi, E. Telatar and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," *IEEE Trans. Inform. Theory*, vol. 63, no. 1, pp. 509–531, January 2017.

[6] L. Yu and V. Y. F. Tan, "Rényi resolvability and its applications to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1862–1897, 2019.

[7] S. Yagli and P. Cuff, "Exact exponent for soft covering,". *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 7635–7654, 2019.

[8] S.-B. Li, K. Li, and L. Yu, "Two-parameter Rényi information quantities with applications to privacy amplification and soft covering," submitted for publication, 2026. Available on-line at: `https://arxiv.org/abs/2511.02297`.

[9] P. Cuff, "A stronger soft-covering lemma and applications," *Proc. 2nd Workshop on Physical-Layer Methods for Wireless Security* (co-located with IEEE CNS), Florence, Italy, pp. 40–43, September 2015.

[10] P. Cuff, "Soft covering with high probability,". in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2963–2967, 2016.

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

[12] N. Weinberger and N. Merhav, "Codeword or noise? Exact random coding exponents for joint detection and decoding," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5077–5094, September 2014.

[13] N. Merhav, "A statistical-physics refinement of soft covering," submitted for publication, 2026. Available on-line at: `https://arxiv.org/pdf/2605.01839`