

The Third-Order Term in the Normal Approximation for the AWGN Channel

Vincent Y. F. Tan

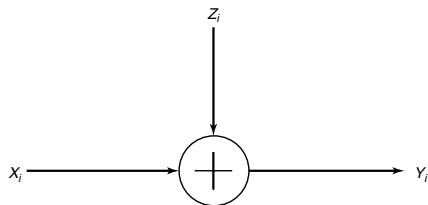
Department of Electrical and Computer Engineering,
Department of Mathematics,
National University of Singapore

Joint work with Marco Tomamichel (CQT, NUS)



July 3, 2014

The AWGN Channel

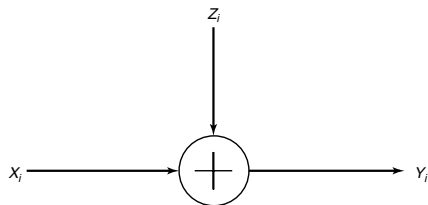


$$Z_i \stackrel{\text{iid}}{\sim} \mathcal{N}(0, 1)$$

$$W(y|x) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(y-x)^2}{2}\right)$$

- The AWGN channel is a well-studied model [Shannon (1948)]

The AWGN Channel



$$Z_i \stackrel{\text{iid}}{\sim} \mathcal{N}(0, 1)$$

$$W(y|x) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(y-x)^2}{2}\right)$$

- The AWGN channel is a well-studied model [Shannon (1948)]
- Assuming an average power constraint

$$\frac{1}{n} \sum_{i=1}^n X_i^2 \leq P$$

the capacity is the familiar expression

$$C(P) = \frac{1}{2} \log(1 + P) \quad \text{bits per ch use}$$

Non-Asymptotic Definition and Strong Converse

- Let

$$M^*(n, \varepsilon, P) := \max\{m \in \mathbb{N} : \exists (n, m, \varepsilon, P)\text{-code}\}$$

Non-Asymptotic Definition and Strong Converse

- Let

$$M^*(n, \varepsilon, P) := \max\{m \in \mathbb{N} : \exists (n, m, \varepsilon, P)\text{-code}\}$$

- (n, m, ε, P) -code: blocklength n , number of codewords m , average error ε and average power P
- We are interested in asymptotic expansion of

$$\log M^*(n, \varepsilon, P) = an + b\sqrt{n} + \text{higher order terms}$$

Non-Asymptotic Definition and Strong Converse

- Let

$$M^*(n, \varepsilon, P) := \max\{m \in \mathbb{N} : \exists (n, m, \varepsilon, P)\text{-code}\}$$

- (n, m, ε, P) -code: blocklength n , number of codewords m , average error ε and average power P
- We are interested in asymptotic expansion of

$$\log M^*(n, \varepsilon, P) = an + b\sqrt{n} + \text{higher order terms}$$

- From Shannon's result and the strong converse (e.g., Shannon (1959), Yoshihara (1964))

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log M^*(n, \varepsilon, P) = C(P), \quad \forall \varepsilon \in (0, 1)$$

Second-Order Asymptotics

- Hayashi (2009) and Polyanskiy-Poor-Verdú (2010) showed the more refined expansion

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \theta_n$$

where $V(P)$ is the Gaussian dispersion function defined as

$$V(P) := \log^2 e \cdot \frac{P(P+2)}{2(P+1)^2}, \quad \text{squared bits per ch use}$$

and $\theta_n = o(\sqrt{n})$.

Second-Order Asymptotics

- Hayashi (2009) and Polyanskiy-Poor-Verdú (2010) showed the more refined expansion

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \theta_n$$

where $V(P)$ is the Gaussian dispersion function defined as

$$V(P) := \log^2 e \cdot \frac{P(P+2)}{2(P+1)^2}, \quad \text{squared bits per ch use}$$

and $\theta_n = o(\sqrt{n})$.

- In fact, Theorem 54 in Polyanskiy-Poor-Verdú (2010) shows that

$$K'(\varepsilon, P) \leq \theta_n \leq \frac{1}{2} \log n + \bar{K}(\varepsilon, P).$$

Second-Order Asymptotics

- Hayashi (2009) and Polyanskiy-Poor-Verdú (2010) showed the more refined expansion

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \theta_n$$

where $V(P)$ is the Gaussian dispersion function defined as

$$V(P) := \log^2 e \cdot \frac{P(P+2)}{2(P+1)^2}, \quad \text{squared bits per ch use}$$

and $\theta_n = o(\sqrt{n})$.

- In fact, Theorem 54 in Polyanskiy-Poor-Verdú (2010) shows that

$$K'(\varepsilon, P) \leq \theta_n \leq \frac{1}{2} \log n + \bar{K}(\varepsilon, P).$$

- Our main contribution is an improvement of the lower bound

Tight Third-Order Asymptotics

Theorem (Tan-Tomamichel (2013))

For all $P > 0$ and $\varepsilon \in (0, 1)$, we have

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + \underline{K}(\varepsilon, P)$$

for some finite number $\underline{K}(\varepsilon, P) \in \mathbb{R}$ for n large enough

Tight Third-Order Asymptotics

Theorem (Tan-Tomamichel (2013))

For all $P > 0$ and $\varepsilon \in (0, 1)$, we have

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

for some finite number $\underline{K}(\varepsilon, P) \in \mathbb{R}$ for n large enough

- Combining this with the upper bound (converse) means that

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + O(1).$$

Tight Third-Order Asymptotics

Theorem (Tan-Tomamichel (2013))

For all $P > 0$ and $\varepsilon \in (0, 1)$, we have

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

for some finite number $\underline{K}(\varepsilon, P) \in \mathbb{R}$ for n large enough

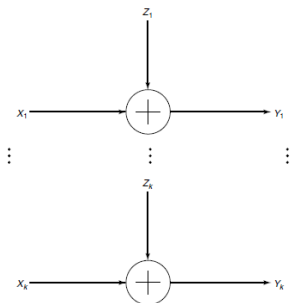
- Combining this with the upper bound (converse) means that

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + O(1).$$

- Converse follows from an application of the hypothesis testing converse by Polyanskiy-Poor-Verdú (2010) or Hayashi-Nagaoka (2003) converse with output distribution

$$Q_{Y^n} = \mathcal{N}(0, P + 1)^{\otimes n}$$

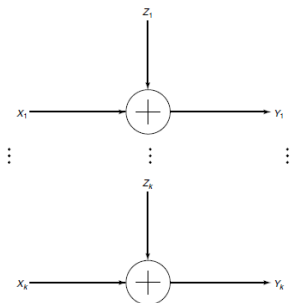
Extensions: Parallel Gaussian Channels



$$Z_{j,i} \stackrel{\text{iid}}{\sim} \mathcal{N}(0, N_j), \quad j = 1, \dots, k$$

Sum of powers equals P

Extensions: Parallel Gaussian Channels



$$Z_{j,i} \stackrel{\text{iid}}{\sim} \mathcal{N}(0, N_j), \quad j = 1, \dots, k$$

Sum of powers equals P

$$\log M^*(n, \varepsilon, P) \geq n \sum_{j=1}^k \mathsf{C}\left(\frac{P_j}{N_j}\right) + \sqrt{n \sum_{j=1}^k \mathsf{V}\left(\frac{P_j}{N_j}\right)} \Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + O(1)$$

where $P_j = |\nu - N_j|^+$ and ν satisfies $\sum_{j=1}^k P_j = P$. Not third-order tight...

Relation to Prefactors for Error Exponents

- For high rates (rates above critical rate), it can be shown following Shannon (1959) that

$$\varepsilon^*(\lfloor \exp(nR) \rfloor, n) = \Theta\left(\frac{\exp(-nE(R))}{n^{(1+|E'(R)|)/2}}\right)$$

where $E(R)$ is the reliability function of the AWGN channel and $E'(R) \leq 0$ is the derivative.

Relation to Prefactors for Error Exponents

- For high rates (rates above critical rate), it can be shown following Shannon (1959) that

$$\varepsilon^*(\lfloor \exp(nR) \rfloor, n) = \Theta\left(\frac{\exp(-nE(R))}{n^{(1+|E'(R)|)/2}}\right)$$

where $E(R)$ is the reliability function of the AWGN channel and $E'(R) \leq 0$ is the derivative.

- Prefactor is

$$\frac{1}{n^{(1+|E'(R)|)/2}}$$

Relation to Prefactors for Error Exponents

- For high rates (rates above critical rate), it can be shown following Shannon (1959) that

$$\varepsilon^*(\lfloor \exp(nR) \rfloor, n) = \Theta\left(\frac{\exp(-nE(R))}{n^{(1+|E'(R)|)/2}}\right)$$

where $E(R)$ is the reliability function of the AWGN channel and $E'(R) \leq 0$ is the derivative.

- Prefactor is

$$\frac{1}{n^{(1+|E'(R)|)/2}}$$

- Some similarities to third-order terms

Comparison of Prefactors to Third-Order Terms

Channel	Third-Order Term	EE Prefactor
AWGN (This Work)	$\frac{1}{2} \log n + O(1)$	$\frac{1}{n^{(1+ E'(R))/2}}$
Non-singular, Symmetric [♥] DMC	$\frac{1}{2} \log n + O(1)$ [◇]	$\frac{1}{n^{(1+ E'(R))/2}}$ [♣]
Singular, Symmetric DMC	$O(1)$ [♠]	$\frac{1}{n^{1/2}}$ [♣]

Comparison of Prefactors to Third-Order Terms

Channel	Third-Order Term	EE Prefactor
AWGN (This Work)	$\frac{1}{2} \log n + O(1)$	$\frac{1}{n^{(1+ E'(R))/2}}$
Non-singular, Symmetric [♥] DMC	$\frac{1}{2} \log n + O(1)$ [◇]	$\frac{1}{n^{(1+ E'(R))/2}}$ [♣]
Singular, Symmetric DMC	$O(1)$ [♠]	$\frac{1}{n^{1/2}}$ [♣]

- ♥ Symmetry not required for third-order term to be $\frac{1}{2} \log n + O(1)$
- ◇ Polyanskiy (2010) and Tomamichel-Tan (2013)

Comparison of Prefactors to Third-Order Terms

Channel	Third-Order Term	EE Prefactor
AWGN (This Work)	$\frac{1}{2} \log n + O(1)$	$\frac{1}{n^{(1+ E'(R))/2}}$
Non-singular, Symmetric [♡] DMC	$\frac{1}{2} \log n + O(1)$ [◇]	$\frac{1}{n^{(1+ E'(R))/2}}$ [♣]
Singular, Symmetric DMC	$O(1)$ [♠]	$\frac{1}{n^{1/2}}$ [♣]

- ♡ Symmetry not required for third-order term to be $\frac{1}{2} \log n + O(1)$
- ◇ Polyanskiy (2010) and Tomamichel-Tan (2013)
- ♣ Altuğ-Wagner (2011-2012), Scarlett *et al.* (2013)
- ♠ Altuğ-Wagner (2013) and Polyanskiy-Poor-Verdú (2010)

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

- Main steps include:

- 1 Random coding union (RCU) bound

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

- Main steps include:
 - 1 Random coding union (RCU) bound
 - 2 Codewords drawn from uniform distribution on sphere

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

- Main steps include:

- 1 Random coding union (RCU) bound
- 2 Codewords drawn from uniform distribution on sphere
- 3 Identification of typical channel outputs

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

- Main steps include:

- 1 Random coding union (RCU) bound
- 2 Codewords drawn from uniform distribution on sphere
- 3 Identification of typical channel outputs
- 4 Probability of log-likelihood falling in a small interval (Laplace approximation)

Proof Strategy

- We want to prove that

$$\log M^*(n, \varepsilon, P) \geq nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2} \log n + \underline{K}(\varepsilon, P)$$

- Main steps include:

- 1 Random coding union (RCU) bound
- 2 Codewords drawn from uniform distribution on sphere
- 3 Identification of typical channel outputs
- 4 Probability of log-likelihood falling in a small interval (Laplace approximation)
- 5 Evaluation of RCU using Berry-Esseen

RCU Bound and Choice of Input Distribution

- RCU bound: For any input distribution P_{X^n} and decoding metric $q(x^n, y^n)$, there exists an (n, M, ε', P) -code satisfying

$$\varepsilon' \leq \mathbb{E} \left[\min \left\{ 1, M \Pr \left(q(\bar{X}^n, Y^n) \geq q(X^n, Y^n) | X^n, Y^n \right) \right\} \right]$$

where $(X^n, \bar{X}^n, Y^n) \sim P_{X^n}(x^n) \times P_{X^n}(\bar{x}^n) \times W^n(y^n|x^n)$

RCU Bound and Choice of Input Distribution

- RCU bound: For any input distribution P_{X^n} and decoding metric $q(x^n, y^n)$, there exists an (n, M, ε', P) -code satisfying

$$\varepsilon' \leq \mathbb{E} \left[\min \left\{ 1, M \Pr \left(q(\bar{X}^n, Y^n) \geq q(X^n, Y^n) | X^n, Y^n \right) \right\} \right]$$

where $(X^n, \bar{X}^n, Y^n) \sim P_{X^n}(x^n) \times P_{X^n}(\bar{x}^n) \times W^n(y^n|x^n)$

- We choose

$$P_{X^n}(x^n) \propto \delta(\|x^n\|_2^2 - nP)$$

the uniform distribution on the power sphere $\{x^n : \|x^n\|_2^2 = nP\}$

RCU Bound and Choice of Input Distribution

- RCU bound: For any input distribution P_{X^n} and decoding metric $q(x^n, y^n)$, there exists an (n, M, ε', P) -code satisfying

$$\varepsilon' \leq \mathbb{E} \left[\min \left\{ 1, M \Pr \left(q(\bar{X}^n, Y^n) \geq q(X^n, Y^n) | X^n, Y^n \right) \right\} \right]$$

where $(X^n, \bar{X}^n, Y^n) \sim P_{X^n}(x^n) \times P_{X^n}(\bar{x}^n) \times W^n(y^n|x^n)$

- We choose

$$P_{X^n}(x^n) \propto \delta(\|x^n\|_2^2 - nP)$$

the uniform distribution on the power sphere $\{x^n : \|x^n\|_2^2 = nP\}$

- Satisfies power constraints

$$\frac{1}{n} \sum_{i=1}^n X_i^2 \leq P$$

with probability one

Decoding Metric

- The decoding metric $q(x^n, y^n)$ is chosen as

$$q(x^n, y^n) := \log \frac{W^n(y^n|x^n)}{P_{X^n} W^n(y^n)}.$$

where $P_{X^n} W^n$ is the output distribution induced by P_{X^n} and W^n

Decoding Metric

- The decoding metric $q(x^n, y^n)$ is chosen as

$$q(x^n, y^n) := \log \frac{W^n(y^n|x^n)}{P_{X^n} W^n(y^n)}.$$

where $P_{X^n} W^n$ is the output distribution induced by P_{X^n} and W^n

- Let the probability within the RCU bound be parametrized as

$$g(t, y^n) := \Pr (q(\bar{X}^n, Y^n) \geq t | Y^n = y^n)$$

then it can be seen by using the definition of q and Bayes rule that

$$g(t, y^n) = \mathbb{E} [\exp(-q(X^n, Y^n)) \mathbb{I}\{q(X^n, Y^n) \geq t\} | Y^n = y^n]$$

- It is imperative to understand the behavior of $q(X^n, Y^n)$

Inner Product and Typical Channel Outputs

- By standard manipulations, we have

$$q(x^n, y^n) = \frac{n}{2} \log \frac{1}{2\pi} + \langle x^n, y^n \rangle - nP - \|y^n\|_2^2 - \log P_{X^n} W^n(y^n)$$

Inner Product and Typical Channel Outputs

- By standard manipulations, we have

$$q(x^n, y^n) = \frac{n}{2} \log \frac{1}{2\pi} + \langle x^n, y^n \rangle - nP - \|y^n\|_2^2 - \log P_{X^n} W^n(y^n)$$

- Since $\frac{1}{n} \|Y^n\|_2^2$ is almost constant with very high probability, we study the statistical properties of

$$\langle X^n, Y^n \rangle$$

where $(X^n, Y^n) \sim P_{X^n} \times W^n$ is not a sequence of iid random variables

Inner Product and Typical Channel Outputs

- By standard manipulations, we have

$$q(x^n, y^n) = \frac{n}{2} \log \frac{1}{2\pi} + \langle x^n, y^n \rangle - nP - \|y^n\|_2^2 - \log P_{X^n} W^n(y^n)$$

- Since $\frac{1}{n} \|Y^n\|_2^2$ is almost constant with very high probability, we study the statistical properties of

$$\langle X^n, Y^n \rangle$$

where $(X^n, Y^n) \sim P_{X^n} \times W^n$ is not a sequence of iid random variables

- We may assume that Y^n is typical in the sense that

$$\frac{1}{n} \|Y^n\|_2^2 \in [P + 1 - \delta_n, P + 1 + \delta_n]$$

and $\delta_n = n^{-1/3}$

Probability of Log-Likelihood in An Interval

Lemma

For y^n typical, the following holds for any a and μ

$$\Pr(q(X^n, Y^n) \in [a, a + \mu] \mid Y^n = y^n) \leq \kappa(P) \cdot \frac{\mu}{\sqrt{n}}.$$

Probability of Log-Likelihood in An Interval

Lemma

For y^n typical, the following holds for any a and μ

$$\Pr(q(X^n, Y^n) \in [a, a + \mu] \mid Y^n = y^n) \leq \kappa(P) \cdot \frac{\mu}{\sqrt{n}}.$$

- Say $\|y^n\|_2^2 = ns$ where $s \in [P + 1 - \delta_n, P + 1 + \delta_n]$. Then we simply have to consider

$$\Pr(\langle X^n, Z^n \rangle \in [b, b + \mu] \mid \|X^n + Z^n\|_2^2 = ns)$$

Probability of Log-Likelihood in An Interval

Lemma

For y^n typical, the following holds for any a and μ

$$\Pr(q(X^n, Y^n) \in [a, a + \mu] \mid Y^n = y^n) \leq \kappa(P) \cdot \frac{\mu}{\sqrt{n}}.$$

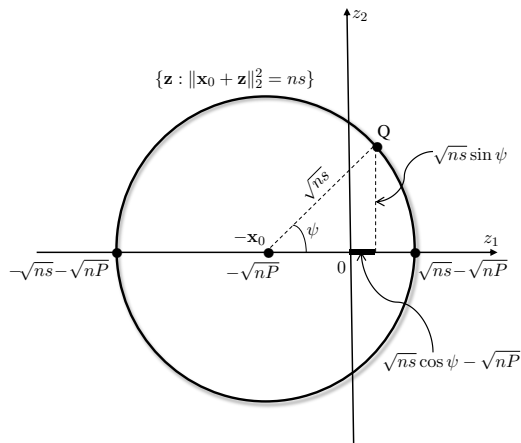
- Say $\|y^n\|_2^2 = ns$ where $s \in [P + 1 - \delta_n, P + 1 + \delta_n]$. Then we simply have to consider

$$\Pr(\langle X^n, Z^n \rangle \in [b, b + \mu] \mid \|X^n + Z^n\|_2^2 = ns)$$

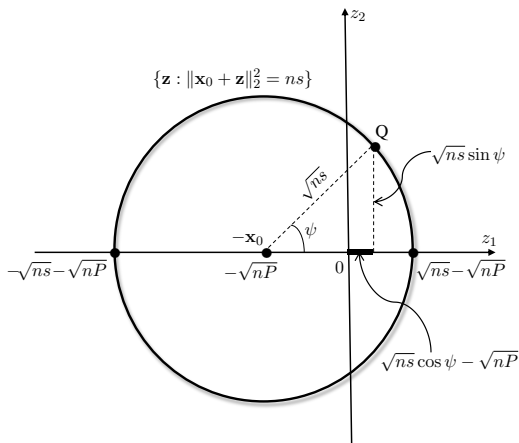
- By spherical symmetry, choose $X^n = x_0^n := (\sqrt{nP}, 0, \dots, 0)$ so

$$\Pr\left(Z_1 + \sqrt{nP} \in \left[\frac{b}{\sqrt{nP}}, \frac{b + \mu}{\sqrt{nP}}\right] \mid \|x_0^n + Z^n\|_2^2 = ns\right)$$

Probability of Log-Likelihood in An Interval



Probability of Log-Likelihood in An Interval



Probability that $Z_1 + \sqrt{nP}$ belongs to an interval of length μ/\sqrt{n} if Z^n lands on the sphere with radius \sqrt{ns} centered at $(-\sqrt{nP}, 0, \dots, 0)$?

Probability of Log-Likelihood in An Interval

- Leverage on radial symmetry
- Change coordinates

$$Z_1 = \sqrt{ns} \cos \Psi - \sqrt{nP}$$

- Apply Laplace approximation for integrals to the conditional probability density of Ψ given Z^n lands on sphere to prove lemma, i.e.,

$$\Pr \left(Z_1 + \sqrt{nP} \in \left[\frac{b}{\sqrt{nP}}, \frac{b + \mu}{\sqrt{nP}} \right] \mid \|x_0^n + Z^n\|_2^2 = ns \right) \leq O \left(\frac{\mu}{\sqrt{n}} \right)$$

Probability of Decoding Metric Exceeding t

- Recall that

$$g(t, y^n) = \Pr(q(\bar{X}^n, Y^n) \geq t \mid Y^n = y^n)$$

- Using the Lemma, we can upper bound $g(t, y^n)$ (uniformly for typical y^n) as

$$g(t, y^n) \leq O\left(\frac{\exp(-t)}{\sqrt{n}}\right).$$

Probability of Decoding Metric Exceeding t

- Recall that

$$g(t, y^n) = \Pr(q(\bar{X}^n, Y^n) \geq t \mid Y^n = y^n)$$

- Using the Lemma, we can upper bound $g(t, y^n)$ (uniformly for typical y^n) as

$$g(t, y^n) \leq O\left(\frac{\exp(-t)}{\sqrt{n}}\right).$$

- The rest of the proof follows by evaluating RCU using Berry-Esseen similar to Theorem 53 in Polyanskiy (2010)

Probability of Decoding Metric Exceeding t

- Recall that

$$g(t, y^n) = \Pr(q(\bar{X}^n, Y^n) \geq t \mid Y^n = y^n)$$

- Using the Lemma, we can upper bound $g(t, y^n)$ (uniformly for typical y^n) as

$$g(t, y^n) \leq O\left(\frac{\exp(-t)}{\sqrt{n}}\right).$$

- The rest of the proof follows by evaluating RCU using Berry-Esseen similar to Theorem 53 in Polyanskiy (2010)
- The \sqrt{n} above contributes to the achievability of the $\frac{1}{2} \log n$ term

Conclusion

- We completed the story up to the third-order for AWGN channels

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + O(1)$$

- We proved the lower bound using some simple calculations and Berry-Esseen theorem

Conclusion

- We completed the story up to the third-order for AWGN channels

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + O(1)$$

- We proved the lower bound using some simple calculations and Berry-Esseen theorem
- Intriguing potential connection between third-order terms and prefactors in the error exponents regime

Conclusion

- We completed the story up to the third-order for AWGN channels

$$\log M^*(n, \varepsilon, P) = nC(P) + \sqrt{nV(P)}\Phi^{-1}(\varepsilon) + \frac{1}{2}\log n + O(1)$$

- We proved the lower bound using some simple calculations and Berry-Esseen theorem
- Intriguing potential connection between third-order terms and prefactors in the error exponents regime
- For detailed derivations, see <http://arxiv.org/abs/1311.2337>