Binary Hypothesis Testing and Sphere-Packing Bounds

Gonzalo Vazquez-Vilar

joint work with

Albert Guillén i Fàbregas

Sergio Verdú

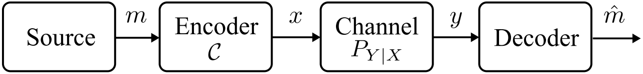
Universidad Carlos III de Madrid

Universitat Pompeu Fabra Barcelona

Princeton University

Workshop on Beyond I.I.D. in Information Theory
July 26, 2017

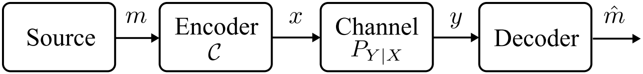
Channel Coding



- Codebook $\mathcal{C} = \{x_1, \ldots, x_M\}$
- Error probability under ML decoding

$$\epsilon(\mathcal{C}) = 1 - \frac{1}{M} \sum_y \max_{x \in \mathcal{C}} P_{Y|X}(y|x)$$

Channel Coding

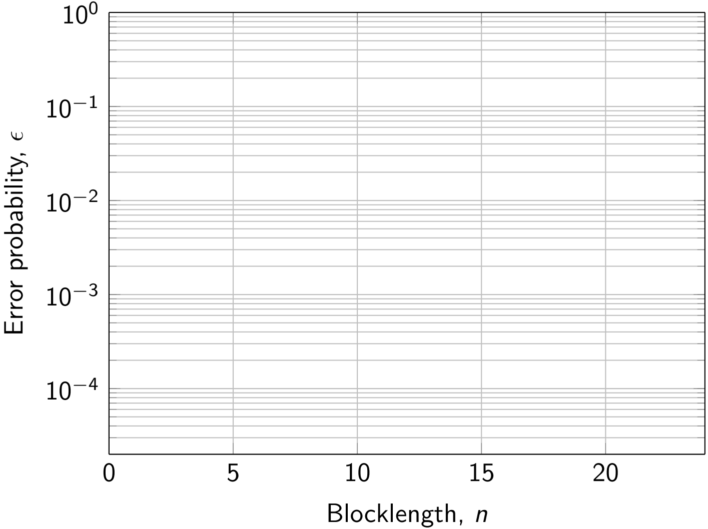


- Codebook $\mathcal{C} = \{x_1, \ldots, x_M\}$

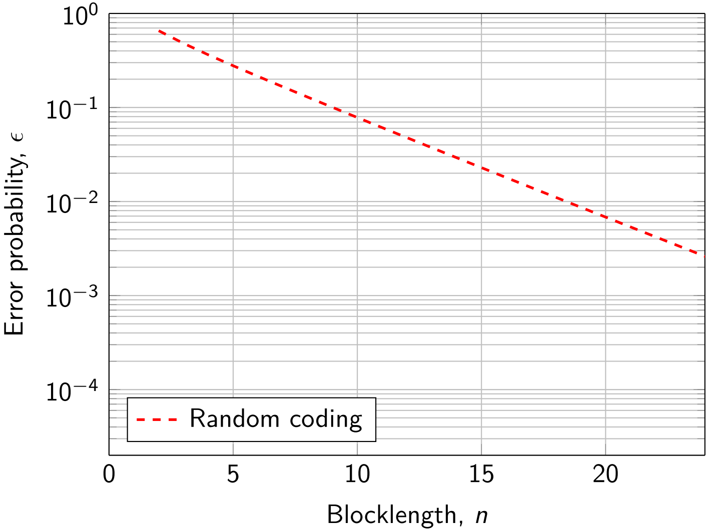
- Error probability under ML decoding

$$\epsilon(\mathcal{C}) = 1 - \frac{1}{M} \sum_y \max_{x \in \mathcal{C}} P_{Y|X}(y|x)$$

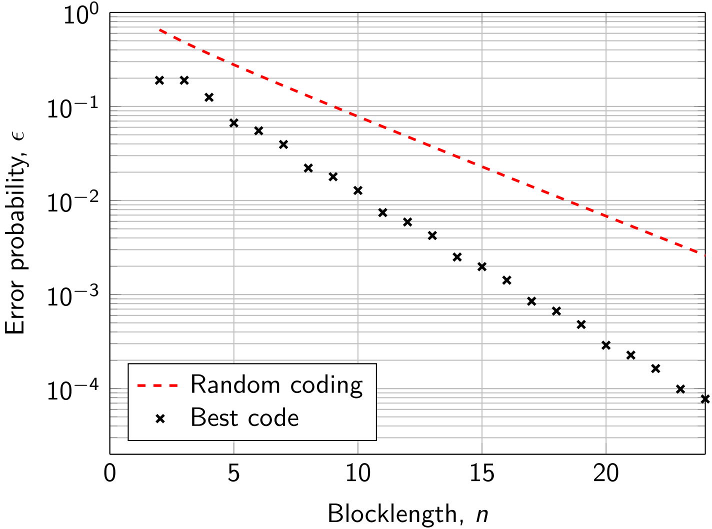
Channel Coding



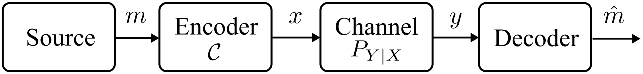
Channel Coding



Channel Coding



Channel Coding



- Error probability under ML decoding

$$\epsilon(\mathcal{C}) = 1 - \frac{1}{M} \sum_{y} \max_{x \in \mathcal{C}} P_{Y|X}(y|x)$$

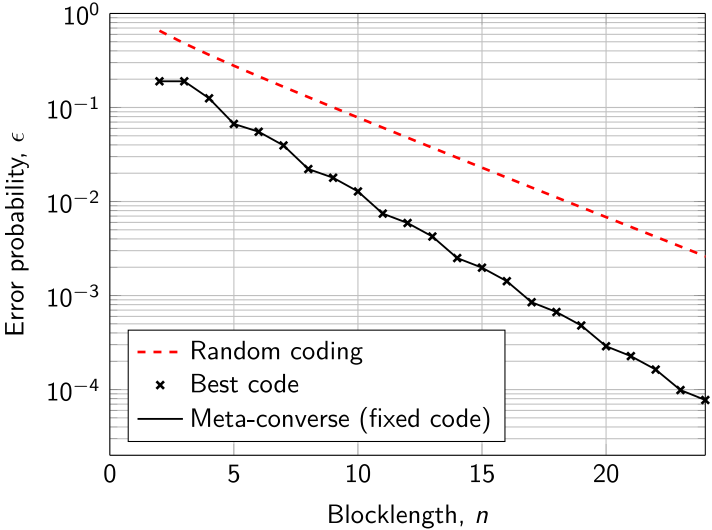
Theorem: Meta-converse[1] is tight[2] (for a fixed code)

$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\}$$

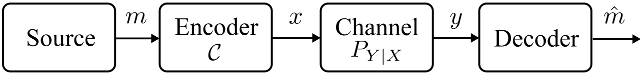
[1] Y. Polyanskiy, H. V. Poor, S. Verdú, **"Channel coding rate in the finite blocklength regime,"** IEEE Trans. Inf. Theory, 2010

[2] G. Vazquez-Vilar, A. Tauste Campo, A. Guillén i Fàbregas, A. Martinez, **"Bayesian M-ary Hypothesis Testing: The Meta-Converse and Verdú-Han Bounds are Tight,"** IEEE Trans. Inf. Theory, 2016

Channel Coding



Channel Coding



- Error probability under ML decoding

$$\epsilon(\mathcal{C}) = 1 - \frac{1}{M} \sum_{y} \max_{x \in \mathcal{C}} P_{Y|X}(y|x)$$

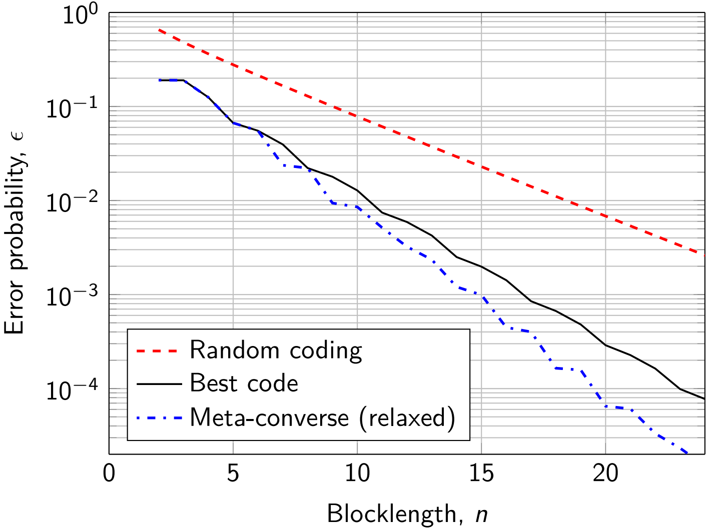
Theorem: Meta-converse, PPV bound, non-signalling converse

$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\}$$

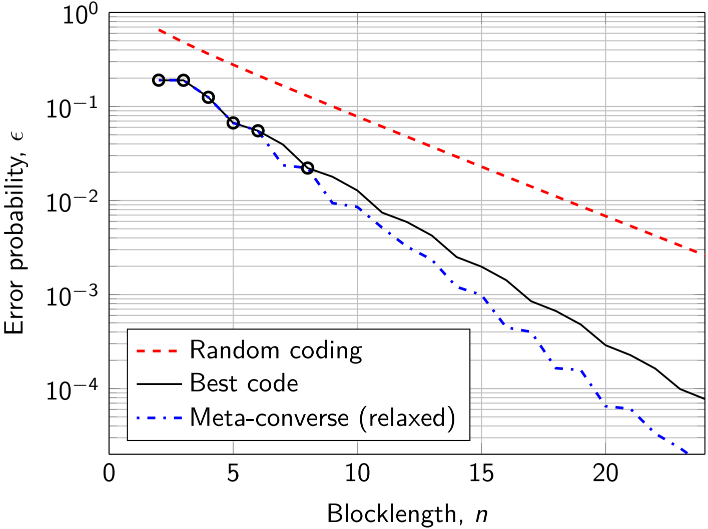
$$\geq \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

Y. Polyanskiy, H. V. Poor, S. Verdú, **"Channel coding rate in the finite blocklength regime,"** IEEE Trans. Inf. Theory, 2010

Channel Coding



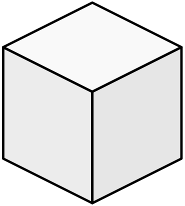
Channel Coding



Outline

- Motivation
- Quantum hypothesis testing
- Quasi-perfect codes
- Sphere-packing bounds

Binary Hypothesis Testing



ρ_0 vs. ρ_1

Optimal trade-off

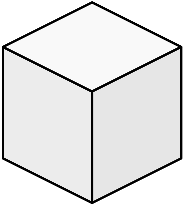
$$\alpha_\beta(\rho_0 \,\|\, \rho_1) \triangleq \min_{0 \le T \le I} \Big\{ \underbrace{1 - \mathrm{Tr}[\rho_0 T]}_{\text{type-0 error}} \;\Big|\; \underbrace{\mathrm{Tr}[\rho_1 T]}_{\text{type-1 error}} \le \beta \Big\}$$

C. W. Helstrom, **"Detection theory and quantum mechanics,"** Inf. and Control, 1967.

P. A. Bakut and S. S. Shchurov, **"Optimal detection of a quantum signal,"** Probl. Peredachi Inf., 1968.

A. S. Holevo, **"An analog of the theory of statistical decisions in noncommutative theory of probability,"** Trudy Moskov. Mat. Obšč., 1972.

Binary Hypothesis Testing



ρ_0 vs. ρ_1

Optimal trade-off

$$\alpha_\beta(\rho_0 \,\|\, \rho_1) \triangleq \min_{0 \le T \le I} \Big\{ \underbrace{1 - \mathrm{Tr}[\rho_0 T]}_{\text{type-0 error}} \;\Big|\; \underbrace{\mathrm{Tr}[\rho_1 T]}_{\text{type-1 error}} \le \beta \Big\}$$

C. W. Helstrom, **"Detection theory and quantum mechanics,"** Inf. and Control, 1967.

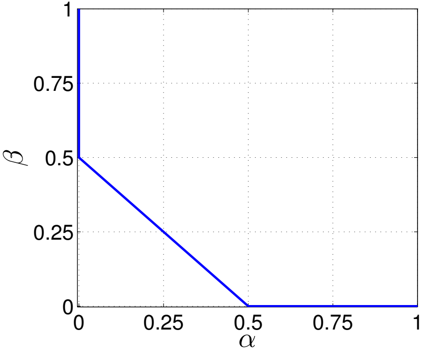
P. A. Bakut and S. S. Shchurov, **"Optimal detection of a quantum signal,"** Probl. Peredachi Inf., 1968.

A. S. Holevo, **"An analog of the theory of statistical decisions in noncommutative theory of probability,"** Trudy Moskov. Mat. Obšč., 1972.

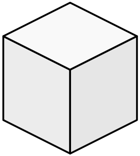
Binary Hypothesis Testing

$$\begin{bmatrix} 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 \end{bmatrix} \quad \text{vs.} \quad \begin{bmatrix} 1/4 & 0 & 0 & 1/4 \\ 0 & 1/4 & 1/4 & 0 \\ 0 & 1/4 & 1/4 & 0 \\ 1/4 & 0 & 0 & 1/4 \end{bmatrix}$$

Optimal trade-off



M-ary Hypothesis Testing



$\tau_1, \dots, \tau_M$
(equiprobable)

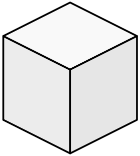
- Measurement

$$\mathcal{M} = \{\Pi_1, \dots, \Pi_M\}$$

- Error probability

$$\epsilon(\mathcal{M}) = 1 - \frac{1}{M} \sum_{i=1}^{M} \mathrm{Tr}[\tau_i \Pi_i]$$

M-ary Hypothesis Testing



$\mathcal{T}_1, \ldots, \mathcal{T}_M$
(equiprobable)

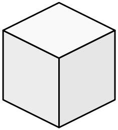
Optimal measurement

$$\epsilon(\mathcal{M}^\star) = \min_{\{\Pi_m\}} \left\{ 1 - \frac{1}{M} \sum_{i=1}^{M} \mathrm{Tr}[\mathcal{T}_i \Pi_i] \;\middle|\; \sum_{i=1}^{M} \Pi_i \leq \boldsymbol{I} \right\}$$

[1]A. S. Holevo, **"Statistical decision theory for quantum systems,"** J. Multivariate Anal. 3, 1973.
[2]H. P. Yuen, R. S. Kennedy, and M. Lax, **"Optimum testing of multiple hypotheses in quantum detection theory,"** IEEE Trans. Inf. Theory, 1975.

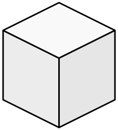
Binary Hypothesis Testing Formulation

M-ary hypothesis test



$\tau_1, \dots, \tau_M$
(equiprobable)

Binary hypothesis test



ρ_0 vs. ρ_1?

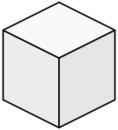
Theorem

$$\epsilon(\mathcal{M}^\star) = \max_{\mu} \alpha_{\frac{1}{M}}\left(\rho_0 \,\|\, \rho_1(\mu)\right)$$

G. Vazquez-Vilar, **"Multiple quantum hypothesis testing and classical-quantum channel converse bounds,"** 2016 IEEE Int. Symp. Inf. Theory

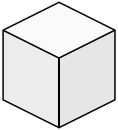
Binary Hypothesis Testing Formulation

M-ary hypothesis test



$\tau_1, \ldots, \tau_M$
(equiprobable)

Binary hypothesis test



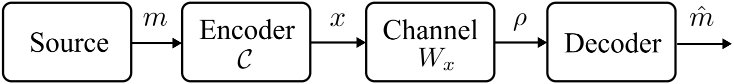
$$\rho_0 \triangleq \tfrac{1}{M}\,\mathrm{diag}\big(\tau_1, \ldots, \tau_M\big)$$
vs.
$$\rho_1(\mu) \triangleq \tfrac{1}{M}\,\mathrm{diag}\big(\mu, \ldots, \mu\big)$$

Theorem

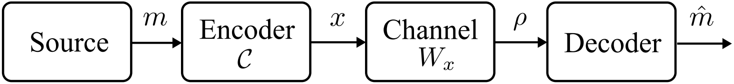
$$\epsilon(\mathcal{M}^\star) = \max_{\mu} \alpha_{\frac{1}{M}}\big(\rho_0 \,\|\, \rho_1(\mu)\big)$$

G. Vazquez-Vilar, **"Multiple quantum hypothesis testing and classical-quantum channel converse bounds,"** 2016 IEEE Int. Symp. Inf. Theory

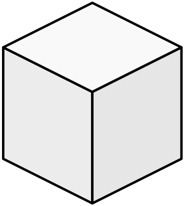
Application to Classical-Quantum Channels



Application to Classical-Quantum Channels

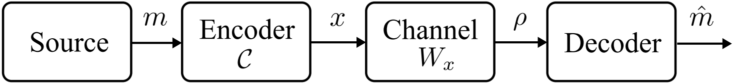


For a fixed code



$W_{x_1}, \ldots, W_{x_M}$?

Application to Classical-Quantum Channels



Corollary: Matthews-Wehner[1] bound is tight[2]

$$\epsilon(\mathcal{C}) = \max_{\mu_0} \alpha_{\frac{1}{M}}\left(\rho_{\mathcal{C}}^{\mathbb{A}\mathbb{B}} \,\middle\|\, \rho_{\mathcal{C}}^{\mathbb{A}} \otimes \mu_0^{\mathbb{B}}\right)$$

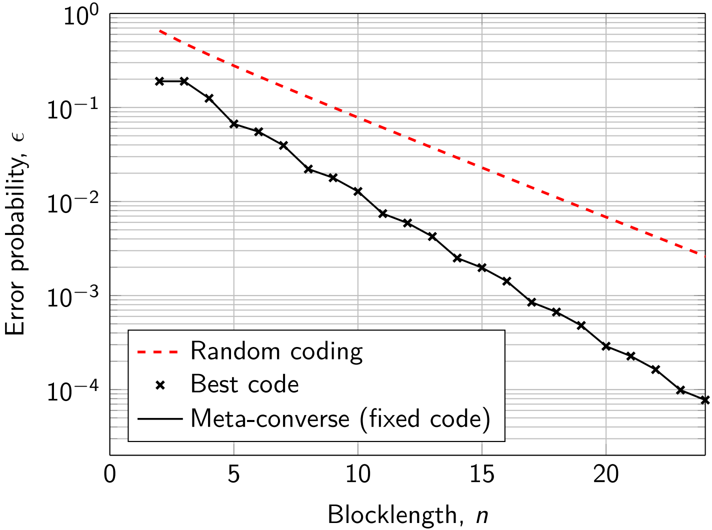
where $\mathbb{A}$ and $\mathbb{B}$ denote the input and out systems, and

$$\rho_{\mathcal{C}}^{\mathbb{A}} = \frac{1}{M}\sum_{x\in\mathcal{C}} |x\rangle\langle x|^{\mathbb{A}}, \qquad \rho_{\mathcal{C}}^{\mathbb{A}\mathbb{B}} = \frac{1}{M}\sum_{x\in\mathcal{C}} |x\rangle\langle x|^{\mathbb{A}} \otimes W_x^{\mathbb{B}}$$

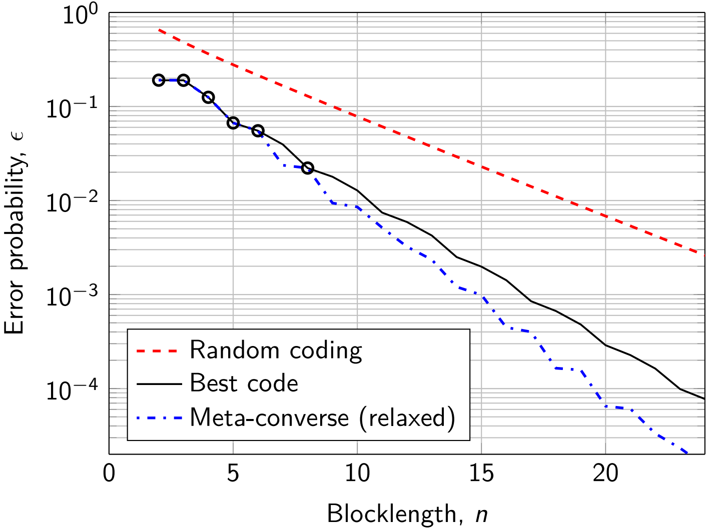
[1] W. Matthews and S. Wehner, **"Finite blocklength converse bounds for quantum channels,"** IEEE Trans. Inf. Theory, 2014.

[2] G. Vazquez-Vilar, **"Multiple quantum hypothesis testing and classical-quantum channel converse bounds,"** 2016 IEEE Int. Symp. Inf. Theory.

Channel Coding



Channel Coding



(Classical) Channel Coding

Theorem

$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\}$$

$$\geq \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

(Classical) Channel Coding

Theorem

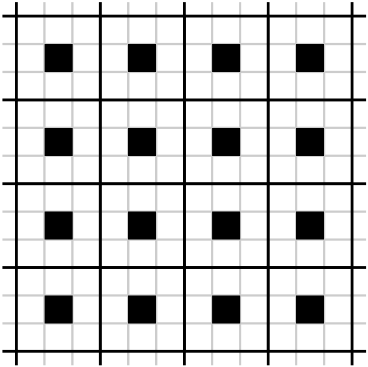
$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\}$$

$$\stackrel{?}{=} \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

Perfect Codes

Definition: Perfect code

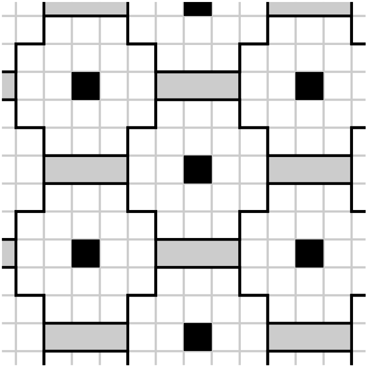
A binary code is said to be *perfect* if non-overlapping Hamming spheres of radius t centered on the codewords exactly fill out the space.



Quasi-Perfect Codes

Definition: Quasi-perfect code

A *quasi-perfect* code is defined as a code in which Hamming spheres of radius t centered on the codewords are non-overlapping and Hamming spheres of radius $t+1$ cover the space, possibly with overlaps.



Generalized Quasi-Perfect Codes

How to **extend quasi-perfect codes** beyond Hamming distance?

- Alternative "spheres"

$$\mathcal{S}_x(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} \geq \theta \right\}$$

- Interior and shell

$$\mathcal{S}_x^{\bullet}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} > \theta \right\}$$

$$\mathcal{S}_x^{\circ}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} = \theta \right\}$$

Generalized Quasi-Perfect Codes

How to **extend quasi-perfect codes** beyond Hamming distance?

- Alternative "spheres"

$$\mathcal{S}_x(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} \geq \theta \right\}$$

- Interior and shell

$$\mathcal{S}_x^{\bullet}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} > \theta \right\}$$

$$\mathcal{S}_x^{\circ}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} = \theta \right\}$$

Generalized Quasi-Perfect Codes

How to **extend quasi-perfect codes** beyond Hamming distance?

- Alternative "spheres"

$$\mathcal{S}_x(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} \geq \theta \right\}$$

- Interior and shell

$$\mathcal{S}_x^{\bullet}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} > \theta \right\}$$

$$\mathcal{S}_x^{\circ}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} = \theta \right\}$$

Generalized Quasi-Perfect Codes

Definition: Generalized perfect code

A code $\mathcal{C}$ is *generalized perfect* if there exists $\theta \in [0,1]$, $Q \in \mathcal{Q}$ such that the codeword-centered "spheres" $\{\mathcal{S}_x(\theta, Q), x \in \mathcal{C}\}$

(i) are disjoint, and

(ii) cover the space.

Definition: Generalized quasi-perfect code

A code $\mathcal{C}$ is *generalized quasi-perfect* if there exists $\theta \in [0,1]$, $Q \in \mathcal{Q}$ such that

(i) the "spheres" $\{\mathcal{S}_x^{\bullet}(\theta, Q), x \in \mathcal{C}\}$ are disjoint, and

(ii) the "spheres" $\{\mathcal{S}_x(\theta, Q), x \in \mathcal{C}\}$ cover the space.

$Q \in \mathcal{Q}$ implies some symmetry conditions on the tilting distribution Q.

Generalized Quasi-Perfect Codes

Definition: Generalized perfect code

A code $\mathcal{C}$ is *generalized perfect* if there exists $\theta \in [0,1]$, $Q \in \mathcal{Q}$ such that the codeword-centered "spheres" $\left\{\mathcal{S}_x(\theta, Q), x \in \mathcal{C}\right\}$

(i) are disjoint, and

(ii) cover the space.

Definition: Generalized quasi-perfect code

A code $\mathcal{C}$ is *generalized quasi-perfect* if there exists $\theta \in [0,1]$, $Q \in \mathcal{Q}$ such that

(i) the "spheres" $\left\{\mathcal{S}_x^{\bullet}(\theta, Q), x \in \mathcal{C}\right\}$ are disjoint, and

(ii) the "spheres" $\left\{\mathcal{S}_x(\theta, Q), x \in \mathcal{C}\right\}$ cover the space.

$Q \in \mathcal{Q}$ implies some symmetry conditions on the tilting distribution Q.

Generalized Quasi-Perfect Codes

Theorem: Relaxed meta-converse is tight (for quasi-perfect codes)[1]

For $P_{Y|X}$ symmetric and $\mathcal{C}$ generalized quasi-perfect, then

$$\epsilon(\mathcal{C}) = \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

- Known for the BSC[2][3]
- For Q uniform, it recovers Hamada's definition[4]
- The new definition includes, e.g., MDS codes for the BEC[1]

[1] G. Vazquez-Vilar, A. Guillén i Fàbregas, S. Verdú, **"Quasi-Perfect Codes via the Meta-Converse,"** in preparation.

[2] Y. Polyanskiy, H. V. Poor, S. Verdú, **"Channel coding rate in the finite blocklength regime,"** IEEE Trans. Inf. Theory, 2010.

[3] R. G. Gallager, **"Information Theory and Reliable Communication,"** John Wiley & Sons, Inc., 1968.

[4] M. Hamada, **"A sufficient condition for a code to achieve the minimum decoding error probability - generalization of perfect and quasi-perfect codes,"** IEICE Trans. on Fund. of Electronics, Comm. and Comp. Sciences, 2000.

Generalized Quasi-Perfect Codes

Theorem: Relaxed meta-converse is tight (for quasi-perfect codes)[1]

For $P_{Y|X}$ symmetric and $\mathcal{C}$ generalized quasi-perfect, then

$$\epsilon(\mathcal{C}) = \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

- Known for the BSC[2][3]
- For Q uniform, it recovers Hamada's definition[4]
- The new definition includes, e.g., MDS codes for the BEC[1]

[1] G. Vazquez-Vilar, A. Guillén i Fàbregas, S. Verdú, **"Quasi-Perfect Codes via the Meta-Converse,"** in preparation.

[2] Y. Polyanskiy, H. V. Poor, S. Verdú, **"Channel coding rate in the finite blocklength regime,"** IEEE Trans. Inf. Theory, 2010.

[3] R. G. Gallager, **"Information Theory and Reliable Communication,"** John Wiley & Sons, Inc., 1968.

[4] M. Hamada, **"A sufficient condition for a code to achieve the minimum decoding error probability - generalization of perfect and quasi-perfect codes,"** IEICE Trans. on Fund. of Electronics, Comm. and Comp. Sciences, 2000.

Key Idea of the Proof

- Neyman-Pearson test of $P_X \times P_{Y|X}$ vs. $P_X \times Q$ is

$$T_{\text{NP}}(0|x,y) = \begin{cases} 1, & \text{if } y \in \mathcal{S}_x^{\bullet}(\theta, Q) \\ p, & \text{if } y \in \mathcal{S}_x^{\circ}(\theta, Q) \\ 0, & \text{otherwise} \end{cases}$$

- The regions of the NP test coincide with the "spheres"

$$\mathcal{S}_x^{\bullet}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} > \theta \right\}$$

$$\mathcal{S}_x^{\circ}(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} = \theta \right\}$$

- Provided certain symmetry conditions, $\epsilon(\mathcal{C})$ coincides with

$$\alpha_{\frac{1}{M}}\left(P_X \times P_{Y|X} \,\|\, P_X \times Q\right)$$

Sphere-packing bounds

Theorem: Relaxed meta-converse

$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\} \tag{1}$$

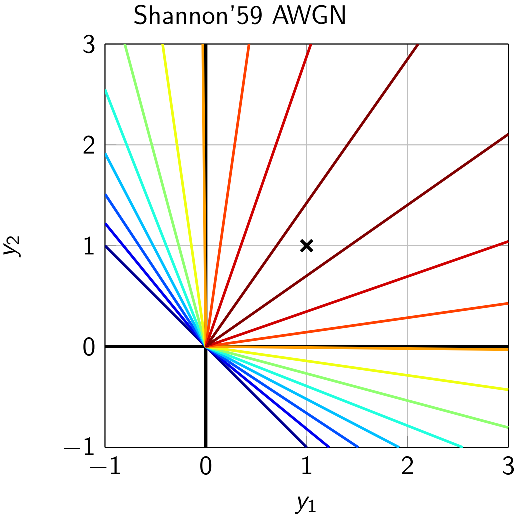
$$\geq \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\} \tag{2}$$

- Eq. (1) retains information about "neighbours" and true decoding regions
- In the relaxation (2) only "spheres" are left

$$\mathcal{S}_x(\theta, Q) \triangleq \left\{ y \in \mathcal{Y} \,\middle|\, \frac{P_{Y|X}(y|x)}{Q(y)} \geq \theta \right\}$$

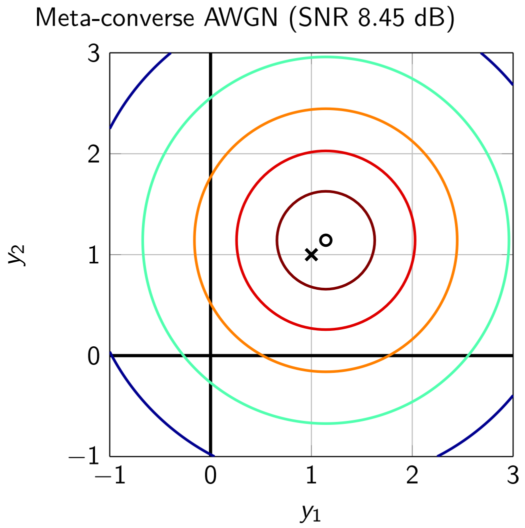
- The relaxed meta-converse is thus a sphere-packing bound
- If the "spheres" coincide with with the decoding regions, it is tight!

How do these spheres look like?



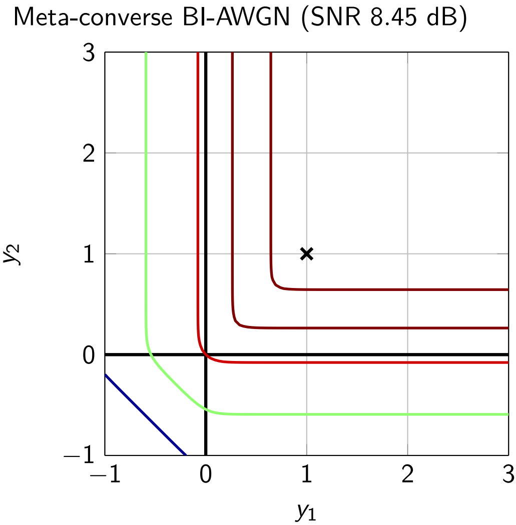
C. E. Shannon, **"Probability of error for optimal codes in a Gaussian channel,"** The Bell System Tech. J., 1959.

How do these spheres look like?

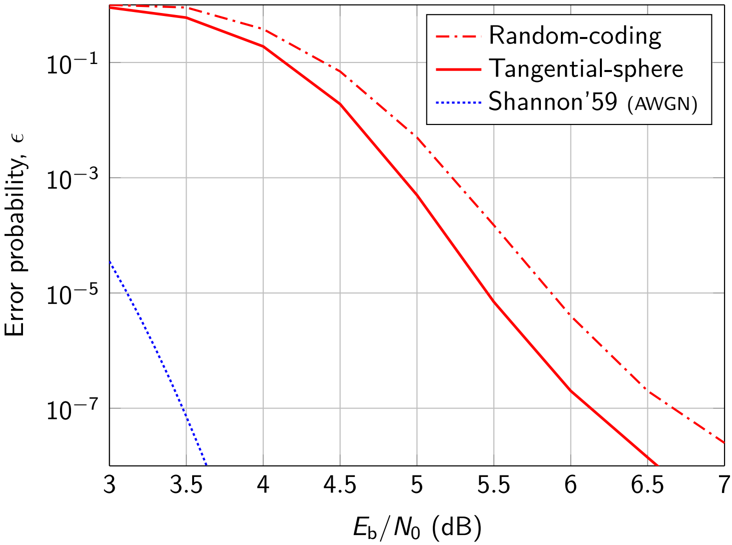


Y. Polyanskiy, H. V. Poor, S. Verdú, **"Channel coding rate in the finite blocklength regime,"** IEEE Trans. Inf. Theory, 2010.

How do these spheres look like?

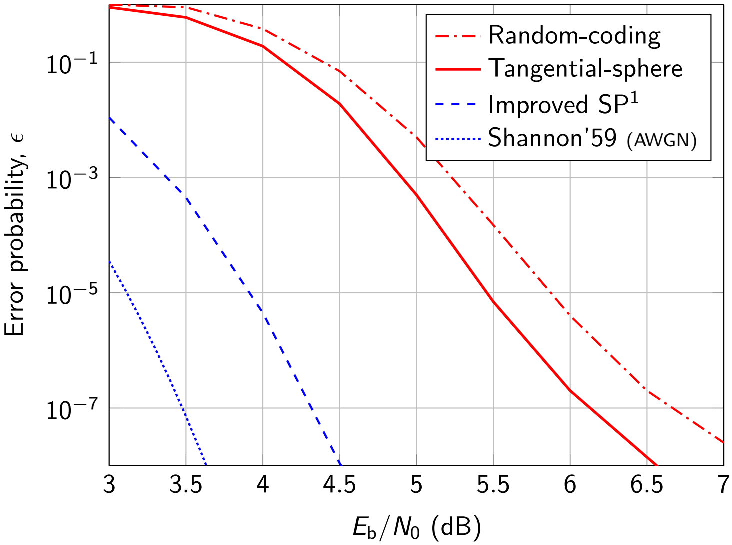


Example: BI-AWGN Channel ($n = 300$, $R = 0.9$)



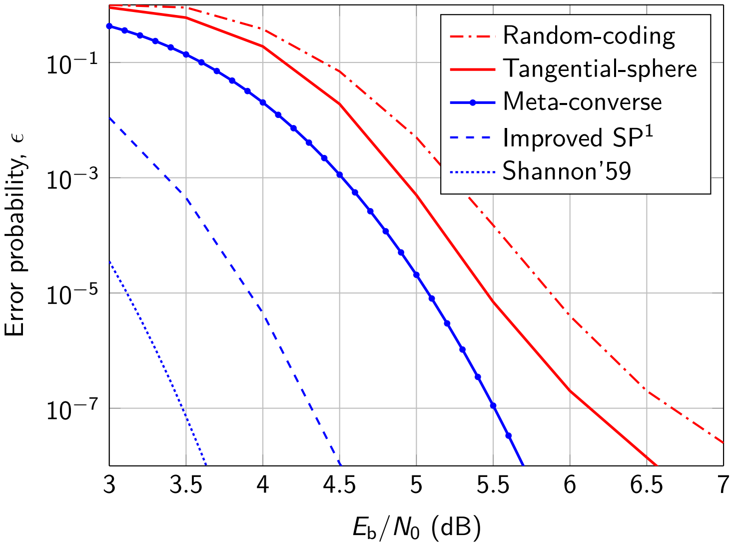
[1] G. Wiechman, I. Sason, **"An improved sphere-packing bound for finite-length codes over symmetric memoryless channels,"** IEEE Trans. Inf. Theory, 2008.

Example: BI-AWGN Channel ($n = 300$, $R = 0.9$)



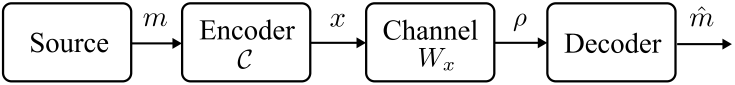
[1] G. Wiechman, I. Sason, **"An improved sphere-packing bound for finite-length codes over symmetric memoryless channels,"** IEEE Trans. Inf. Theory, 2008.

Example: BI-AWGN Channel ($n = 300$, $R = 0.9$)



[1] G. Wiechman, I. Sason, **"An improved sphere-packing bound for finite-length codes over symmetric memoryless channels,"** IEEE Trans. Inf. Theory, 2008.

Spheres in Classical-Quantum Channels?



- According to the Neyman-Pearson lemma the "sphere" is now

$$\mathcal{S}_x(t,\mu) \triangleq \{W_x - t\mu \geq 0\}$$
$$\mathcal{S}_x^{\bullet}(t,\mu) \triangleq \{W_x - t\mu > 0\}$$

Definition: Quantum quasi-perfect code

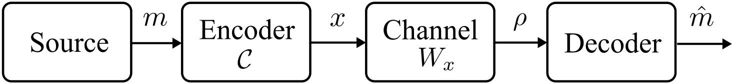
A code $\mathcal{C}$ is *generalized quasi-perfect* if there exists μ, $t \geq 0$ such that

(i) the projectors $\{\mathcal{S}_x^{\bullet}(t,\mu), x \in \mathcal{C}\}$ are orthogonal to each other,

(ii) the projectors $\{\mathcal{S}_x(t,\mu), x \in \mathcal{C}\}$ cover the space, i.e.,

$$\sum_{x\in\mathcal{C}} \mathcal{S}_x(t,\mu) \geq \boldsymbol{I}.$$

Spheres in Classical-Quantum Channels?



- According to the Neyman-Pearson lemma the "sphere" is now

$$\mathcal{S}_x(t,\mu) \triangleq \{W_x - t\mu \geq 0\}$$
$$\mathcal{S}_x^{\bullet}(t,\mu) \triangleq \{W_x - t\mu > 0\}$$

Definition: Quantum quasi-perfect code

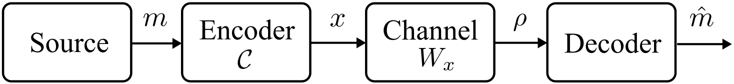
A code $\mathcal{C}$ is *generalized quasi-perfect* if there exists μ, $t \geq 0$ such that

(i) the projectors $\{\mathcal{S}_x^{\bullet}(t,\mu), x \in \mathcal{C}\}$ are orthogonal to each other,

(ii) the projectors $\{\mathcal{S}_x(t,\mu), x \in \mathcal{C}\}$ cover the space, i.e.,

$$\sum_{x \in \mathcal{C}} \mathcal{S}_x(t,\mu) \geq \boldsymbol{I}.$$

Spheres in Classical-Quantum Channels?



- According to the Neyman-Pearson lemma the "sphere" is now

$$\mathcal{S}_x(t,\mu) \triangleq \{W_x - t\mu \geq 0\}$$
$$\mathcal{S}_x^{\bullet}(t,\mu) \triangleq \{W_x - t\mu > 0\}$$

Definition: Quantum quasi-perfect code

A code $\mathcal{C}$ is *generalized quasi-perfect* if there exists μ, $t \geq 0$ such that

(i) the projectors $\left\{\mathcal{S}_x^{\bullet}(t,\mu), x \in \mathcal{C}\right\}$ are orthogonal to each other,

(ii) the projectors $\left\{\mathcal{S}_x(t,\mu), x \in \mathcal{C}\right\}$ cover the space, i.e.,

$$\sum_{x \in \mathcal{C}} \mathcal{S}_x(t,\mu) \geq \boldsymbol{I}.$$

Wrap Up

Original problem	Equivalent problem
M-ary hypothesis testing	Binary hypothesis testing

Theorem

$$\begin{aligned}\epsilon(\mathcal{C}) &= \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\} \\ &\geq \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}\end{aligned}$$

With equality if $\mathcal{C}$ is *quasi-perfect* with respect to W_x

Wrap Up

Original problem	Equivalent problem
M-ary hypothesis testing	Binary hypothesis testing

Theorem

$$\epsilon(\mathcal{C}) = \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X^{\mathcal{C}} \times P_{Y|X} \,\|\, P_X^{\mathcal{C}} \times Q \right) \right\}$$
$$\geq \inf_{P_X} \max_{Q} \left\{ \alpha_{\frac{1}{M}} \left(P_X \times P_{Y|X} \,\|\, P_X \times Q \right) \right\}$$

With equality if $\mathcal{C}$ is *quasi-perfect* with respect to W_x