

局所差分プライバシーと その量子拡張における最適化入門

吉田 裕哉

2026 年 10 月 11 日

第 10 回すうがく徒のつどい

前提知識: ($\mathbb{R}^d$ と $\mathbb{C}^d$ に関する) 線型代数

【今日の目標】聴衆が次の内容を理解することを目指す:

- ① 最適化問題の定式化,
- ② Kairouz らの一般論,
- ③ ①の量子拡張.

①-③について話した後,

- ④ 最近の研究

について話す.

※文献情報については, アブストラクトまたは [arXiv:2605.27278](https://arxiv.org/abs/2605.27278) を参照.

目次

- ① 問題背景から最適化問題の定式化まで
- ② Kairouz らの一般論
- ③ 最適化問題の量子拡張
- ④ 最近の研究

目次

- ① 問題背景から最適化問題の定式化まで
- ② Kairouz らの一般論
- ③ 最適化問題の量子拡張
- ④ 最近の研究

$$\text{最適化問題} = \underbrace{\text{制約条件 (定義域)}}_{\text{プライバシー保護}} + \underbrace{\text{目的関数}}_{\text{有用性}}.$$

- 目的 1: 各個人は私的データ X (犯罪歴や病歴など) を知られたくない.
- 目的 2: データ解析者は X に関する統計的な情報 (平均や割合など) を公開データ Y から推定するため, 推定精度を最大にしたい.

$$\begin{array}{ccc} X & \xrightarrow[\mathbb{P}_{Y|X}]{\text{randomize}} & Y \\ \text{in } \mathcal{X} & & \text{in } \mathcal{Y} \end{array} \xrightarrow{\text{release}}$$

- 目的 1 を達成するために, $\underbrace{q = \mathbb{P}_{Y|X}}_{\text{変数}}$ に局所差分プライバシーを課す.

局所差分プライバシー (local differential privacy, LDP)

$$\varepsilon\text{-LDP: } \forall x, x' \in \mathcal{X}, \forall y \in \mathcal{Y}, \quad q(y|x') \leq e^\varepsilon q(y|x).$$

- 有限個の線型不等式.¹
- プライバシー損失の上界を正のパラメータ ε で表す.

例:

$$q_2^* = [q_2^*(y|x)]_{y,x \in \{1,2\}} = \begin{bmatrix} q_2^*(1|1) & q_2^*(1|2) \\ q_2^*(2|1) & q_2^*(2|2) \end{bmatrix} = \frac{1}{e^\varepsilon + 1} \begin{bmatrix} e^\varepsilon & 1 \\ 1 & e^\varepsilon \end{bmatrix}.$$

注意. 条件付き確率分布は列確率行列とみなせる:

$$q = [q(y|x)]_{y \in \mathcal{Y}, x \in \mathcal{X}}.$$

¹この講演では常に $2 \leq |\mathcal{X}|, |\mathcal{Y}| < \infty$ である.

有用性関数 (utility function)

- q の実数値関数. この講演では $\Phi_C(q)$ と表す.
- 通常は以下の DPI が成り立つことを仮定する.

データ処理不等式 (data processing inequality, DPI)

任意の ε -LDP メカニズム q と,² 任意の列確率行列 Λ に対して,

$$\Phi_C(\Lambda q) \leq \Phi_C(q).$$

$$(\Lambda q)_{z,x} = \sum_{y \in \mathcal{Y}} \Lambda(z|y) q(y|x).$$

²LDP の文脈では, 変数 q をメカニズムと呼ぶ.

- 記号. $[k] := \{1, 2, \dots, k\}$.
- 今後は, 整数 $n, d \geq 2$ を用いて, $\mathcal{X} = [n]$ かつ $\mathcal{Y} = [d]$ とする.
- 注意. q の各列ベクトルは確率ベクトル.

$$q = [p_1, \dots, p_n], \quad p_1, \dots, p_n \in \mathbb{R}^d.$$

最適化問題 (古典)

整数 $n \geq 2$ と実数 $\varepsilon > 0$ を固定する.

$$\text{OPT}_n(\varepsilon; \Phi_C) := \underbrace{\sup_{q: \varepsilon\text{-LDP}}}_{\text{Privacy protection}} \underbrace{\Phi_C(q)}_{\text{Utility}}.$$

ただし, 整数 $d \geq 2$ は固定しない.

目次

- ① 問題背景から最適化問題の定式化まで
- ② Kairouz らの一般論
- ③ 最適化問題の量子拡張
- ④ 最近の研究

Assumption 1 (only in this section)

Assume that Φ_C is of the form

$$\Phi_C(q) = \Phi_C(p_1, \dots, p_n) = \sum_{\substack{y \in [d] \\ p_1(y), \dots, p_n(y) > 0}} \phi(p_1(y), \dots, p_n(y)),$$

where $\phi: (0, \infty)^n \rightarrow \mathbb{R}$ is *sublinear*:

- $\phi(\alpha \mathbf{z}) = \alpha \phi(\mathbf{z})$ for every $\alpha > 0$ and every $\mathbf{z} \in (0, \infty)^n$;
- $\phi(\mathbf{z} + \mathbf{z}') \leq \phi(\mathbf{z}) + \phi(\mathbf{z}')$ for all $\mathbf{z}, \mathbf{z}' \in (0, \infty)^n$.

Assumption 1 (only in this section)

Assume that Φ_C is of the form

$$\Phi_C(q) = \Phi_C(p_1, \dots, p_n) = \sum_{\substack{y \in [d] \\ p_1(y), \dots, p_n(y) > 0}} \phi(p_1(y), \dots, p_n(y)),$$

where $\phi: (0, \infty)^n \rightarrow \mathbb{R}$ is *sublinear*:

- $\phi(\alpha \mathbf{z}) = \alpha \phi(\mathbf{z})$ for every $\alpha > 0$ and every $\mathbf{z} \in (0, \infty)^n$;
- $\phi(\mathbf{z} + \mathbf{z}') \leq \phi(\mathbf{z}) + \phi(\mathbf{z}')$ for all $\mathbf{z}, \mathbf{z}' \in (0, \infty)^n$.

Then Φ_C satisfies the DPI [Kairouz et al., 2016]:

$$\Phi_C(\Lambda q) \leq \Phi_C(q)$$

for every ε -LDP mechanism q and every column-stochastic matrix Λ .

Notation. Denote by $\mathbb{1}_n$ the all-ones column vector in $\mathbb{R}^n$.

Theorem 1 (Kairouz et al., 2016)

The classical optimal value $\text{OPT}_n(\varepsilon; \Phi_C)$ is equal to the maximum of the sum

$$\sum_{\mathbf{z} \in \{0,1\}^n} \phi(\mathbb{1}_n + (e^\varepsilon - 1)\mathbf{z})\alpha_{\mathbf{z}} \quad (1)$$

subject to the following constraints.

- ① $\alpha_{\mathbf{z}} \geq 0$ for every $\mathbf{z} \in \{0,1\}^n$.
- ② $\sum_{\mathbf{z} \in \{0,1\}^n} \alpha_{\mathbf{z}}(\mathbb{1}_n + (e^\varepsilon - 1)\mathbf{z}) = \mathbb{1}_n$.

Notation. Denote by $\mathbb{1}_n$ the all-ones column vector in $\mathbb{R}^n$.

Theorem 1 (Kairouz et al., 2016)

The classical optimal value $\text{OPT}_n(\varepsilon; \Phi_C)$ is equal to the maximum of the sum

$$\sum_{\mathbf{z} \in \{0,1\}^n} \phi(\mathbb{1}_n + (e^\varepsilon - 1)\mathbf{z})\alpha_{\mathbf{z}} \quad (1)$$

subject to the following constraints.

- ① $\alpha_{\mathbf{z}} \geq 0$ for every $\mathbf{z} \in \{0,1\}^n$.
- ② $\sum_{\mathbf{z} \in \{0,1\}^n} \alpha_{\mathbf{z}}(\mathbb{1}_n + (e^\varepsilon - 1)\mathbf{z}) = \mathbb{1}_n$.

Eq. (1) is equal to $\Phi_C(Q_\alpha)$, where $Q_\alpha(\mathbf{z}|i) := \alpha_{\mathbf{z}}(1 + (e^\varepsilon - 1)z_i)$.

If $n = 2$, then

$$\alpha = (\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}) \quad \text{and} \quad Q_\alpha = \text{diag}(\alpha) \begin{bmatrix} 1 & 1 \\ 1 & e^\varepsilon \\ e^\varepsilon & 1 \\ e^\varepsilon & e^\varepsilon \end{bmatrix}.$$

As pointed out in [Holohan et al., 2017],³ one can slightly improve Theorem 1:

$$\{0, 1\}^n \xrightarrow{\text{shrink}} \{0, 1\}^n \setminus \{0^n, 1^n\}.$$

Example. Suppose $n = 2$. Eq. (1) is equal to $\Phi_C(q_2^*)$, since

$$\underbrace{\text{diag}(\alpha_{01}, \alpha_{10}) \begin{bmatrix} 1 & e^\varepsilon \\ e^\varepsilon & 1 \end{bmatrix}}_{\text{Column-stochastic matrix}} = \frac{1}{e^\varepsilon + 1} \begin{bmatrix} 1 & e^\varepsilon \\ e^\varepsilon & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{Permutation matrix}} q_2^*.$$

By this and Theorem 1, $\text{OPT}_2(\varepsilon; \Phi_C) = \Phi_C(q_2^*)$.

³N. Holohan, D. J. Leith, and O. Mason. Extreme points of the local differential privacy polytope. *Linear Algebra Appl.*, 534:78–96, 2017.

As pointed out in [Holohan et al., 2017],³ one can slightly improve Theorem 1:

$$\{0, 1\}^n \xrightarrow{\text{shrink}} \{0, 1\}^n \setminus \{0^n, 1^n\}.$$

Example. Suppose $n = 2$. Eq. (1) is equal to $\Phi_C(q_2^*)$, since

$$\underbrace{\text{diag}(\alpha_{01}, \alpha_{10}) \begin{bmatrix} 1 & e^\varepsilon \\ e^\varepsilon & 1 \end{bmatrix}}_{\text{Column-stochastic matrix}} = \frac{1}{e^\varepsilon + 1} \begin{bmatrix} 1 & e^\varepsilon \\ e^\varepsilon & 1 \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{\text{Permutation matrix}} q_2^*.$$

By this and Theorem 1, $\text{OPT}_2(\varepsilon; \Phi_C) = \Phi_C(q_2^*)$.

Remark. In Theorem 1, it suffices to consider a smaller subclass of Q_α if Φ_C is invariant under a group action [Nam et al., 2026, preprint].

³N. Holohan, D. J. Leith, and O. Mason. Extreme points of the local differential privacy polytope. *Linear Algebra Appl.*, 534:78–96, 2017.

目次

- ① 問題背景から最適化問題の定式化まで
- ② Kairouz らの一般論
- ③ 最適化問題の量子拡張**
- ④ 最近の研究

- ① A *classical state* is a probability vector p :

$$p \in [0, \infty)^d, \quad \sum_{i=1}^d p(i) = 1.$$

- ② A *quantum state* is a density matrix ρ :

$$\rho \in \text{PSD}(d), \quad \text{Tr } \rho = 1.$$

- ③ Classical state $p \xrightarrow{\text{embed}}$ Quantum state $\text{diag}(p)$.

Unit vector $|u\rangle \in \mathbb{C}^d \xrightarrow{\text{represented as}}$ Density matrix $|u\rangle\langle u|$.

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \xrightarrow{\text{represented as}} \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

- 古典: $q = [p_1, \dots, p_n]$. 古典状態 $p_1, \dots, p_n$ からなる.
- 量子: $\vec{\rho} = (\rho_1, \dots, \rho_n)$. 量子状態 $\rho_1, \dots, \rho_n$ からなる.

量子局所差分プライバシー (QLDP)

$$\varepsilon\text{-QLDP: } \forall x, x' \in \mathcal{X}, \quad \rho_{x'} \leq e^\varepsilon \rho_x.$$

- LDP の量子拡張の 1 つ. 有限個の線型行列不等式.⁴
- プライバシー損失の上界を正のパラメータ ε で表す.

⁴行列不等式は両辺の差が半正定値であることを意味する. $\mathcal{X} = [n]$ であることに注意.

- 古典: $q = [p_1, \dots, p_n]$. 古典状態 $p_1, \dots, p_n$ からなる.
- 量子: $\vec{\rho} = (\rho_1, \dots, \rho_n)$. 量子状態 $\rho_1, \dots, \rho_n$ からなる.

量子局所差分プライバシー (QLDP)

$$\varepsilon\text{-QLDP: } \forall x, x' \in \mathcal{X}, \quad \rho_{x'} \leq e^\varepsilon \rho_x.$$

- LDP の量子拡張の 1 つ. 有限個の線型行列不等式.⁴
- プライバシー損失の上界を正のパラメータ ε で表す.

Φ_C の量子拡張

$\Phi_Q(\vec{\rho})$ を次の条件を満たす $\vec{\rho}$ の実数値関数とする.

- $\Phi_C = \Phi_Q|_{\text{diag}}$.
- 任意のユニタリ行列 U と任意の ε -QLDP メカニズム $\vec{\rho}$ に対して,

$$\Phi_Q(U\rho_1U^\dagger, \dots, U\rho_nU^\dagger) = \Phi_Q(\vec{\rho}).$$

⁴行列不等式は両辺の差が半正定値であることを意味する. $\mathcal{X} = [n]$ であることに注意.

- 古典: $q = [p_1, \dots, p_n]$. 古典状態 $p_1, \dots, p_n$ からなる.
- 量子: $\vec{\rho} = (\rho_1, \dots, \rho_n)$. 量子状態 $\rho_1, \dots, \rho_n$ からなる.

最適化問題 (量子)

整数 $n \geq 2$ と実数 $\varepsilon > 0$ を固定する.

$$\text{OPT}_n(\varepsilon; \Phi_Q) := \underbrace{\sup_{\vec{\rho}: \varepsilon\text{-QLDP}}}_{\text{Privacy protection}} \underbrace{\Phi_Q(\vec{\rho})}_{\text{Utility}}.$$

ただし, 整数 $d \geq 2$ (行列サイズ $d \times d$) は固定しない.

目次

- ① 問題背景から最適化問題の定式化まで
- ② Kairouz らの一般論
- ③ 最適化問題の量子拡張
- ④ 最近の研究

Aim 1: To establish a quantum counterpart of Theorem 1

Setting	Class of mechanisms	Utility functions
Classical	Extremal mechanisms Q_α	$\Phi_C = \sum_y \phi(\dots)$
Quantum	?	?
Setting	Privacy regime (range of ε)	References
Classical	All ($\varepsilon > 0$)	[Kairouz et al., 2016]
Quantum		

Aim 1: To establish a quantum counterpart of Theorem 1

Setting	Class of mechanisms	Utility functions
Classical	Extremal mechanisms Q_α	$\Phi_C = \sum_y \phi(\dots)$
Quantum	?	?
Setting	Privacy regime (range of ε)	References
Classical	All ($\varepsilon > 0$)	[Kairouz et al., 2016]
Quantum		

Why is quantum extension difficult?

- Classical: [ratios of entries](#)

$$e^{-\varepsilon} \leq \frac{q(y|x')}{q(y|x)} \leq e^{\varepsilon}, \quad \frac{Q_\alpha(\mathbf{z}|j)}{Q_\alpha(\mathbf{z}|i)} \in \{1, e^{\pm\varepsilon}\}.$$

Aim 1: To establish a quantum counterpart of Theorem 1

Setting	Class of mechanisms	Utility functions
Classical	Extremal mechanisms Q_α	$\Phi_C = \sum_y \phi(\dots)$
Quantum	?	?
Setting	Privacy regime (range of ε)	References
Classical	All ($\varepsilon > 0$)	[Kairouz et al., 2016]
Quantum		

Why is quantum extension difficult?

- Classical: **ratios of entries**

$$e^{-\varepsilon} \leq \frac{q(y|x')}{q(y|x)} \leq e^{\varepsilon}, \quad \frac{Q_\alpha(\mathbf{z}|j)}{Q_\alpha(\mathbf{z}|i)} \in \{1, e^{\pm\varepsilon}\}.$$

- Quantum: **eigenvalues** and **eigenspaces**

$$e^{-\varepsilon} I_d \leq \rho_x^{-1/2} \rho_{x'} \rho_x^{-1/2} \leq e^{\varepsilon} I_d,$$

where I_d is the identity matrix on $\mathbb{C}^d$.

Aim 2: To compare the classical and quantum optimal values

It is clear that

$$\text{OPT}_n(\varepsilon; \Phi_C) \leq \text{OPT}_n(\varepsilon; \Phi_Q).$$

⁵Both $\text{OPT}_n(\varepsilon; \Phi_C)$ and $\text{OPT}_n(\varepsilon; \Phi_Q)$ are determined.

Aim 2: To compare the classical and quantum optimal values

It is clear that

$$\text{OPT}_n(\varepsilon; \Phi_C) \leq \text{OPT}_n(\varepsilon; \Phi_Q).$$

Conditions	' $\leq$ '	Utility functions	References
$n = 2$ and $\varepsilon > 0$	' $=$ '	All	[Y. & Hayashi, 2020] ⁵
$n \geq 3$ and $\varepsilon > 0$	' $<$ '	Minimum of pairwise RLD Fisher info.	[Y., 2025] ⁵
$n \in \{3, 4, \dots, 9\}$ and $\varepsilon \rightarrow +0$	' $<$ '	Error exponent(s) in hypothesis testing	[Nam et al., 2026]
$n \geq 3$ and $\varepsilon \rightarrow +0$	' $<$ '	Error exponents, RLD, and Holevo info., etc.	[Y., 2026+] ⁵

⁵Both $\text{OPT}_n(\varepsilon; \Phi_C)$ and $\text{OPT}_n(\varepsilon; \Phi_Q)$ are determined.

Aim 2: To compare the classical and quantum optimal values

It is clear that

$$\text{OPT}_n(\varepsilon; \Phi_C) \leq \text{OPT}_n(\varepsilon; \Phi_Q).$$

Conditions	' $\leq$ '	Utility functions	References
$n = 2$ and $\varepsilon > 0$	' $=$ '	All	[Y. & Hayashi, 2020] ⁵
$n \geq 3$ and $\varepsilon > 0$	' $<$ '	Minimum of pairwise RLD Fisher info.	[Y., 2025] ⁵
$n \in \{3, 4, \dots, 9\}$ and $\varepsilon \rightarrow +0$	' $<$ '	Error exponent(s) in hypothesis testing	[Nam et al., 2026]
$n \geq 3$ and $\varepsilon \rightarrow +0$	' $<$ '	Error exponents, RLD, and Holevo info., etc.	[Y., 2026+] ⁵

[Y., 2026+]: If $n \geq 3$, then

$$\lim_{\varepsilon \rightarrow +0} \frac{\text{OPT}_n(\varepsilon; \Phi_Q)}{\text{OPT}_n(\varepsilon; \Phi_C)} = \frac{n(n-1)}{2 \lfloor n/2 \rfloor \lceil n/2 \rceil} \geq \frac{3}{2}.$$

⁵Both $\text{OPT}_n(\varepsilon; \Phi_C)$ and $\text{OPT}_n(\varepsilon; \Phi_Q)$ are determined.

Setting	Class of mechanisms	Utility functions
Classical	Extremal mechanisms Q_α	$\Phi_C = \sum_y \phi(\dots)$
Quantum	Isoclinic mechanisms $\vec{\sigma}$	(omitted)
Setting	Privacy regime (range of ε)	References
Classical	All ($\varepsilon > 0$)	[Kairouz et al., 2016]
Quantum	High-privacy regime ($\varepsilon \rightarrow +0$)	[Y., 2026+]

Isoclinic mechanisms: $\vec{\sigma} = (\sigma_1, \dots, \sigma_n)$.

$$\sigma_i := \frac{\mu}{d} I_d + \frac{1 - \mu}{r} P_i.$$

Here, $\{P_i\}_{i \in [n]}$ is an **EITFF $_{\mathbb{C}}(d, r, n)$** , and μ is defined as ... (omitted).

Equi-isoclinic tight fusion frames (EITFFs)

- For $k \in \mathbb{N}$, denote by $[k]$ the set $\{1, 2, \dots, k\}$.
- Let $n, d \in \mathbb{Z}_{\geq 2}$ and $r \in [d - 1]$.

Definition 1 (Theorem 5.2 [Fickus et al., 2017])

We say that a set $\{P_i\}_{i \in [n]}$ of n rank- r orthogonal projections on $\mathbb{C}^d$ is an EITFF if it satisfies the following conditions.

- ① $\sum_{i \in [n]} P_i = (nr/d)I_d$.
- ② There exists $c \in [0, 1]$ such that $P_j P_i P_j = c P_j$ for all $i \neq j$.

Denote by $\text{EITFF}_{\mathbb{C}}(d, r, n)$ an EITFF with parameters d , r , and n .

Equi-isoclinic tight fusion frames (EITFFs)

- For $k \in \mathbb{N}$, denote by $[k]$ the set $\{1, 2, \dots, k\}$.
- Let $n, d \in \mathbb{Z}_{\geq 2}$ and $r \in [d - 1]$.

Definition 1 (Theorem 5.2 [Fickus et al., 2017])

We say that a set $\{P_i\}_{i \in [n]}$ of n rank- r orthogonal projections on $\mathbb{C}^d$ is an EITFF if it satisfies the following conditions.

- ① $\sum_{i \in [n]} P_i = (nr/d)I_d$.
- ② There exists $c \in [0, 1]$ such that $P_j P_i P_j = c P_j$ for all $i \neq j$.

Denote by $\text{EITFF}_{\mathbb{C}}(d, r, n)$ an EITFF with parameters d , r , and n .

- $(n, 1, n)$: an orthonormal basis of $\mathbb{R}^n$ or $\mathbb{C}^n$
- $(n - 1, 1, n)$: n unit vectors in $\mathbb{R}^{n-1}$ forming the vertices of a regular simplex centered at the origin
- $(d, 1, d^2)$: a SIC-POVM (Zauner's conjecture)

Equi-isoclinic tight fusion frames (EITFFs)

Set of values r/d :

$$\mathcal{Q}_n := \{r/d : \text{an EITFF}_{\mathbb{C}}(d, r, n) \text{ exists}\}.$$

- $\mathcal{Q}_n \subset [1/n, 1/2]$.
- $1/n \in \mathcal{Q}_n$ and $1/2 \in \mathcal{Q}_n$ [Fickus et al., 2025].

Equi-isoclinic tight fusion frames (EITFFs)

Set of values r/d :

$$\mathcal{Q}_n := \{r/d : \text{an EITFF}_{\mathbb{C}}(d, r, n) \text{ exists}\}.$$

- $\mathcal{Q}_n \subset [1/n, 1/2]$.
- $1/n \in \mathcal{Q}_n$ and $1/2 \in \mathcal{Q}_n$ [Fickus et al., 2025].
- By [Iverson & O, 2025, preprint] and some existing results,

$$\mathcal{Q}_2 = \{1/2\}, \quad \mathcal{Q}_3 = \{1/3, 1/2\}, \quad \mathcal{Q}_4 = \{1/4, 1/3, 1/2\}, \quad \text{and} \\ \mathcal{Q}_5 = \{1/5, 1/4, 1/3, 2/5, 1/2\}.$$

Equi-isoclinic tight fusion frames (EITFFs)

Set of values r/d :

$$\mathcal{Q}_n := \{r/d : \text{an EITFF}_{\mathbb{C}}(d, r, n) \text{ exists}\}.$$

- $\mathcal{Q}_n \subset [1/n, 1/2]$.
- $1/n \in \mathcal{Q}_n$ and $1/2 \in \mathcal{Q}_n$ [Fickus et al., 2025].
- By [Iverson & O, 2025, preprint] and some existing results,

$$\mathcal{Q}_2 = \{1/2\}, \quad \mathcal{Q}_3 = \{1/3, 1/2\}, \quad \mathcal{Q}_4 = \{1/4, 1/3, 1/2\}, \quad \text{and} \\ \mathcal{Q}_5 = \{1/5, 1/4, 1/3, 2/5, 1/2\}.$$

- These sets can be expressed as $\bigcup_{m=2}^n \mathcal{C}_m$, where

$$\mathcal{C}_m := \{k/m : k \in [1, m/2] \cap \mathbb{Z}\}.$$

However, this is not the case for $n = 12$, since an $\text{EITFF}_{\mathbb{C}}(16, 5, 12)$ exists [Fickus et al., 2026, preprint].

Comparison of two optimal values

- Let Ψ_Q be the error exponent in asymmetric hypothesis testing:

$$\Psi_Q(\vec{\rho}) = \min_{x \in [n]} D(\rho_x \| \rho_{\text{avg}}),$$

where $\rho_{\text{avg}} := (1/n) \sum_{i \in [n]} \rho_i$.

Comparison of two optimal values

- Let Ψ_Q be the error exponent in asymmetric hypothesis testing.

Comparison of two optimal values

- Let Ψ_Q be the error exponent in asymmetric hypothesis testing.
- The classical and isoclinic optimal values can be expressed as

$$\text{OPT}_n(\varepsilon; \Psi_C) = \max_{u \in \mathcal{C}_n} G_{\text{asym}}^C(u), \quad \text{OPT}_n(\varepsilon; \Psi_Q|_{\text{iso}}) = \sup_{u \in \mathcal{Q}_n} G_{\text{asym}}^{\text{iso}}(u).$$

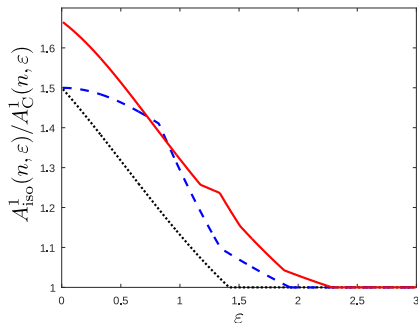
	Classical	Isoclinic
Functions	$G_{\text{asym}}^C(u) \leq G_{\text{asym}}^{\text{iso}}(u)$	$\forall u \in [1/n, 1/2]$
Domains	$\mathcal{C}_n \subset \mathcal{Q}_n$	$\forall n \in \{2, 3, 4, 5, 6\}$

Comparison of two optimal values

- Let Ψ_Q be the error exponent in asymmetric hypothesis testing.
- The classical and isoclinic optimal values can be expressed as

$$\text{OPT}_n(\varepsilon; \Psi_C) = \max_{u \in \mathcal{C}_n} G_{\text{asym}}^C(u), \quad \text{OPT}_n(\varepsilon; \Psi_Q|_{\text{iso}}) = \sup_{u \in \mathcal{Q}_n} G_{\text{asym}}^{\text{iso}}(u).$$

	Classical	Isoclinic
Functions	$G_{\text{asym}}^C(u) \leq G_{\text{asym}}^{\text{iso}}(u)$	$\forall u \in [1/n, 1/2]$
Domains	$\mathcal{C}_n \subset \mathcal{Q}_n$	$\forall n \in \{2, 3, 4, 5, 6\}$



$$\frac{A_{\text{iso}}^1(n, \varepsilon)}{A_C^1(n, \varepsilon)} = \frac{\text{OPT}_n(\varepsilon; \Psi_Q|_{\text{iso}})}{\text{OPT}_n(\varepsilon; \Psi_C)}.$$

$n = 3$, $n = 4$, and $n = 5$.

Summary

$$\mathcal{Q}_n := \{r/d : \text{an EITFF}_{\mathbb{C}}(d, r, n) \text{ exists}\},$$

$$\mathcal{C}_n := \{k/n : k \in [1, n/2] \cap \mathbb{Z}\}.$$

- ① $\text{OPT}_n(\varepsilon; \Phi_C) \xrightarrow{\text{reduce}} \text{Linear program}$ [Kairouz et al., 2016].
- ② $\text{OPT}_2(\varepsilon; \Phi_C) = \text{OPT}_2(\varepsilon; \Phi_Q)$ [Y. & Hayashi, 2020].
- ③ [Y., 2026+]: If $n \geq 3$, then

$$\lim_{\varepsilon \rightarrow +0} \frac{\text{OPT}_n(\varepsilon; \Psi_Q)}{\text{OPT}_n(\varepsilon; \Psi_C)} = \frac{n(n-1)}{2\lfloor n/2 \rfloor \lceil n/2 \rceil} \geq \frac{3}{2}.$$

- ④ EITFFs $\rightarrow$ Isoclinic mechanisms.

Comparison of $\text{OPT}_n(\varepsilon; \Psi_C)$ and $\text{OPT}_n(\varepsilon; \Psi_Q|_{\text{iso}})$

$\rightarrow$ Conjecture $\mathcal{C}_n \subset \mathcal{Q}_n$.

Open problems. ① $\mathcal{C}_n \subset \mathcal{Q}_n$? ② $\text{OPT}_n(\varepsilon; \Phi_Q) = \text{OPT}_n(\varepsilon; \Phi_Q|_{\text{iso}})$?

Other open problems: Section 6 of arXiv:2605.27278.