Around Dvoretzky theorem in quantum information theory

Guillaume AUBRUN

Université Lyon 1, France

Dvoretzky theorem

If $K \subset \mathbf{R}^n$ is a convex body, let $\|x\|_K = \inf\{t > 0 \text{ s.t. } x \in tK\}$.

Theorem (V. Milman)

Let $K \subset \mathbf{R}^n$ or be a convex body and X a random vector uniformly distributed on S^{n-1}. Let $M = \mathbf{E}\|X\|_K$ and $b = \sup \|X\|_K$. Then with high probability, a random k-dimensional subpsace $E \subset \mathbf{R}^n$ satisfies

$$\forall x \in E \cap S^{n-1}, \quad (1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M,$$

with $k = \lfloor c\varepsilon^2 n(M/b)^2 \rfloor$.

- Probability is given on the Grassman manifold is the Haar measure.
- Also true for unit balls of complex normed spaces.
- Combined with the fact that every convex body has an affine image for which $M/b \geqslant \sqrt{\log n}/\sqrt{n}$, this shows that every convex body has a $\lfloor c\varepsilon^2 \log n \rfloor$-dimensional section which is $(1+\varepsilon)$-Euclidean.

Dvoretzky theorem

If $K \subset \mathbf{R}^n$ is a convex body, let $\|x\|_K = \inf\{t > 0 \text{ s.t. } x \in tK\}$.

Theorem (V. Milman)

Let $K \subset \mathbf{R}^n$ or be a convex body and X a random vector uniformly distributed on S^{n-1}. Let $M = \mathbf{E}\|X\|_K$ and $b = \sup \|X\|_K$. Then with high probability, a random k-dimensional subpsace $E \subset \mathbf{R}^n$ satisfies

$$\forall x \in E \cap S^{n-1}, \quad (1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M,$$

with $k = \lfloor c\varepsilon^2 n(M/b)^2 \rfloor$.

- Probability is given on the Grassman manifold is the Haar measure.
- Also true for unit balls of complex normed spaces.
- Combined with the fact that every convex body has an affine image for which $M/b \geqslant \sqrt{\log n}/\sqrt{n}$, this shows that every convex body has a $\lfloor c\varepsilon^2 \log n \rfloor$-dimensional section which is $(1+\varepsilon)$-Euclidean.

Dvoretzky theorem

If $K \subset \mathbf{R}^n$ is a convex body, let $\|x\|_K = \inf\{t > 0 \text{ s.t. } x \in tK\}$.

Theorem (V. Milman)

Let $K \subset \mathbf{R}^n$ or be a convex body and X a random vector uniformly distributed on S^{n-1}. Let $M = \mathbf{E}\|X\|_K$ and $b = \sup \|X\|_K$. Then with high probability, a random k-dimensional subpsace $E \subset \mathbf{R}^n$ satisfies

$$\forall x \in E \cap S^{n-1}, \quad (1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M,$$

with $k = \lfloor c\varepsilon^2 n(M/b)^2 \rfloor$.

- Probability is given on the Grassman manifold is the Haar measure.
- Also true for unit balls of complex normed spaces.
- Combined with the fact that every convex body has an affine image for which $M/b \geqslant \sqrt{\log n}/\sqrt{n}$, this shows that every convex body has a $\lfloor c\varepsilon^2 \log n \rfloor$-dimensional section which is $(1+\varepsilon)$-Euclidean.

Dvoretzky theorem : sketch of proof

Theorem (V. Milman)

Let $K \subset \mathbf{R}^n$ be a convex body and X a random vector uniformly distributed on S^{n-1}. Let $M(K) := \mathbf{E}\|X\|_K$ and $b(K) = \sup \|X\|_K$. Then with high probability, a random k-dimensional subpsace $E \subset \mathbf{R}^n$ satisfies

$$\forall x \in E \cap S^{n-1}, \quad (1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M,$$

with $k = \lfloor c\varepsilon^2 n(M/b)^2 \rfloor$.

1. Concentration on measure on the sphere implies that the proportion of $x \in S^{n-1}$ satisfying

$$(1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M$$

is $1 - \exp(-ck)$.

2. A ε-net in a k-dimensional sphere containts $(1/\varepsilon)^{ck}$ points.

Dvoretzky theorem : sketch of proof

Theorem (V. Milman)

Let $K \subset \mathbf{R}^n$ be a convex body and X a random vector uniformly distributed on S^{n-1}. Let $M(K) := \mathbf{E}\|X\|_K$ and $b(K) = \sup \|X\|_K$. Then with high probability, a random k-dimensional subpsace $E \subset \mathbf{R}^n$ satisfies

$$\forall x \in E \cap S^{n-1}, \quad (1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M,$$

with $k = \lfloor c\varepsilon^2 n (M/b)^2 \rfloor$.

1. Concentration on measure on the sphere implies that the proportion of $x \in S^{n-1}$ satisfying
$$(1-\varepsilon)M \leqslant \|x\|_K \leqslant (1+\varepsilon)M$$
is $1 - \exp(-ck)$.
2. A ε-net in a k-dimensional sphere containts $(1/\varepsilon)^{ck}$ points.

Dvoretzky theorem (continued)

How to compute $M(K)$?

- Let X be uniformly distributed on the sphere, and let G be a $N(0, \mathrm{Id}_n)$ random vector.
  Then $G/|G|$
  1. is independent of $|G|$,
  2. has the same distribution as X.
- Therefore,

$$M(K) = \mathbf{E}\|X\|_K = \frac{\mathbf{E}\|G\|_K}{\mathbf{E}|G|} = \frac{\mathbf{E}\|G\|_K}{\gamma_n}.$$

with $\gamma_n := \mathbf{E}|G|$; one checks that $\sqrt{n-1} \leqslant \gamma_n \leqslant \sqrt{n}$.

Dvoretzky theorem (continued)

How to compute $M(K)$?

- Let X be uniformly distributed on the sphere, and let G be a $N(0, \mathrm{Id}_n)$ random vector.
  Then $G/|G|$
  1. is independent of $|G|$,
  2. has the same distribution as X.
- Therefore,

$$M(K) = \mathbf{E}\|X\|_K = \frac{\mathbf{E}\|G\|_K}{\mathbf{E}|G|} = \frac{\mathbf{E}\|G\|_K}{\gamma_n}.$$

with $\gamma_n := \mathbf{E}|G|$; one checks that $\sqrt{n-1} \leqslant \gamma_n \leqslant \sqrt{n}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n(M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of* ℓ_1^n *?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n(M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of ℓ_1^n ?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n(M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of* ℓ_1^n *?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n (M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of* ℓ_1^n *?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n(M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of ℓ_1^n ?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in ℓ_1^n

Let $\|x\|_1 = \sum |x_i|$ and B_1^n be the unit ball of $\ell_1^n = (\mathbf{R}^n, \|\cdot\|_1)$.

1. $b(B_1^n) = \sqrt{n}$ because $\|\cdot\|_1 \leqslant \sqrt{n}\|\cdot\|_2$.
2. $M(B_1^n) = \frac{n\mathbf{E}|N(0,1)|}{\gamma_n} \sim \frac{cn}{\sqrt{n}} \sim c\sqrt{n}$

So the Dvoretzky dimension of ℓ_1^n is $k = c\varepsilon^2 n(M/b)^2 \sim c\varepsilon^2 n$.

Question

Is there an **explicit** *Dvoretzky subspace of ℓ_1^n ?*

Progress in this direction

- Schechtman : E spanned by i.i.d. ± 1 vectors (n^2 random bits).
- Artstein–Milman, Lovett–Sodin, Guruswami–Lee–Widgerson : construction using very few randomness (n^δ random bits for any $\delta > 0$).
- Indyk : explicit embedding of ℓ_2^k into $\ell_1^{k^{O(\log k)}}$.

Dvoretzky theorem in S_∞^d

Let $\mathbf{K} = \mathbf{R}$ or $\mathbf{C}$, and $\mathcal{M}(\mathbf{K}^d, \mathbf{K}^n)$ be the space of $d \times n$ matrices, equipped with the Hilbert–Schmidt inner product

$$\langle A, B \rangle = \operatorname{Tr} A^* B \qquad \|A\|_{HS} = \sqrt{\operatorname{Tr} A^* A}.$$

Let S_∞^d be the space $\mathcal{M}(\mathbf{K}^d)$ with the operator norm $\|\cdot\|_{op}$.

1. $b(S_\infty^d) = 1$ since $\|\cdot\|_{op} \leqslant \|\cdot\|_{HS}$.
2. $M(S_\infty^d) \sim \frac{1}{d}\mathbf{E}\|G\|_{op}$, where G is a random matrix with i.i.d. $N(0,1)$ entries.
3. Standard results on random matrices assert that $\mathbf{E}\|G\|_{op} \leqslant C\sqrt{d}$,

Therefore the Dvoretzky dimension of S_∞^d is $k = c\varepsilon^2 d^2 (M/b)^2 = c\varepsilon^2 d$ (in a d^2-dimensional space).

Dvoretzky theorem in S_∞^d

Let $\mathbf{K} = \mathbf{R}$ or $\mathbf{C}$, and $\mathcal{M}(\mathbf{K}^d, \mathbf{K}^n)$ be the space of $d \times n$ matrices, equipped with the Hilbert–Schmidt inner product

$$\langle A, B \rangle = \operatorname{Tr} A^* B \qquad \|A\|_{HS} = \sqrt{\operatorname{Tr} A^* A}.$$

Let S_∞^d be the space $\mathcal{M}(\mathbf{K}^d)$ with the operator norm $\|\cdot\|_{op}$.

1. $b(S_\infty^d) = 1$ since $\|\cdot\|_{op} \leqslant \|\cdot\|_{HS}$.
2. $M(S_\infty^d) \sim \frac{1}{d}\mathbf{E}\|G\|_{op}$, where G is a random matrix with i.i.d. $N(0,1)$ entries.
3. Standard results on random matrices assert that $\mathbf{E}\|G\|_{op} \leqslant C\sqrt{d}$,

Therefore the Dvoretzky dimension of S_∞^d is $k = c\varepsilon^2 d^2 (M/b)^2 = c\varepsilon^2 d$ (in a d^2-dimensional space).

Dvoretzky theorem in S_∞^d (continued)

A random $c(\varepsilon)d$-dimensional subspace of S_∞^d is $(1+\varepsilon)$-Euclidean.

Problem

Find explicit Dvoretzky subspaces of S_∞^d.

In the complex case, this would be presumably useful for quantum information theory.

Misleading example : S_∞^d contains obvious d-dimensional 1-Euclidean subspaces : consider matrices with nonzero entries only in the first row. For such a matrix A we have $\|A\|_{op} = \|A\|_{HS}$, while on Dvoretzky subspaces we have $\|A\|_{op} \approx \|A\|_{HS}/\sqrt{d}$.

Dvoretzky theorem in S_∞^d (continued)

A random $c(\varepsilon)d$-dimensional subspace of S_∞^d is $(1+\varepsilon)$-Euclidean.

Problem

Find explicit Dvoretzky subspaces of S_∞^d.

In the complex case, this would be presumably useful for quantum information theory.

Misleading example : S_∞^d contains obvious d-dimensional 1-Euclidean subspaces : consider matrices with nonzero entries only in the first row. For such a matrix A we have $\|A\|_{op} = \|A\|_{HS}$, while on Dvoretzky subspaces we have $\|A\|_{op} \approx \|A\|_{HS}/\sqrt{d}$.

Slepian's lemma

Lemma (Slepian's lemma)

If $K \subset \mathbf{R}^n$ and $\Phi : K \to \mathbf{R}^p$ is a (nonlinear) contraction, then

$$\mathbf{E} \max_{y \in \Phi(K)} \langle g_p, y \rangle \leqslant \mathbf{E} \max_{x \in K} \langle g_n, x \rangle,$$

where g_n is a standard n-dimensional Gaussian vector.

The map $x \oplus y \mapsto x \otimes y$ is the contraction on $S^{d-1} \times S^{d-1}$,

$$|x \otimes y - x' \otimes y'| \leqslant \left(|x - x'|^2 + |y - y'|^2\right)^{1/2}. \tag{1}$$

Since

$$\|G\|_{op} = \sup_{|x|=|y|=1} \langle Gx, y \rangle = \sup_{|x|=|y|=1} \langle G, x \otimes y \rangle,$$

Slepian inequality implies that

$$\mathbf{E}\|G\|_{op} \leqslant 2\gamma_d \leqslant 2\sqrt{d}$$

Slepian's lemma

Lemma (Slepian's lemma)

If $K \subset \mathbf{R}^n$ and $\Phi : K \to \mathbf{R}^p$ is a (nonlinear) contraction, then

$$\mathbf{E} \max_{y \in \Phi(K)} \langle g_p, y \rangle \leqslant \mathbf{E} \max_{x \in K} \langle g_n, x \rangle,$$

where g_n is a standard n-dimensional Gaussian vector.

The map $x \oplus y \mapsto x \otimes y$ is the contraction on $S^{d-1} \times S^{d-1}$,

$$|x \otimes y - x' \otimes y'| \leqslant \left(|x - x'|^2 + |y - y'|^2 \right)^{1/2}. \tag{1}$$

Since

$$\|G\|_{op} = \sup_{|x|=|y|=1} \langle Gx, y \rangle = \sup_{|x|=|y|=1} \langle G, x \otimes y \rangle,$$

Slepian inequality implies that

$$\mathbf{E}\|G\|_{op} \leqslant 2\gamma_d \leqslant 2\sqrt{d}$$

Slepian's lemma

Lemma (Slepian's lemma)

If $K \subset \mathbf{R}^n$ and $\Phi : K \to \mathbf{R}^p$ is a (nonlinear) contraction, then

$$\mathbf{E} \max_{y \in \Phi(K)} \langle g_p, y \rangle \leqslant \mathbf{E} \max_{x \in K} \langle g_n, x \rangle,$$

where g_n is a standard n-dimensional Gaussian vector.

The map $x \oplus y \mapsto x \otimes y$ is the contraction on $S^{d-1} \times S^{d-1}$,

$$|x \otimes y - x' \otimes y'| \leqslant \left(|x - x'|^2 + |y - y'|^2 \right)^{1/2}. \tag{1}$$

Since

$$\|G\|_{op} = \sup_{|x|=|y|=1} \langle Gx, y \rangle = \sup_{|x|=|y|=1} \langle G, x \otimes y \rangle,$$

Slepian inequality implies that

$$\mathbf{E}\|G\|_{op} \leqslant 2\gamma_d \leqslant 2\sqrt{d}$$

Slepian's lemma

Lemma (Slepian's lemma)

If $K \subset \mathbf{R}^n$ and $\Phi : K \to \mathbf{R}^p$ is a (nonlinear) contraction, then

$$\mathbf{E} \max_{y \in \Phi(K)} \langle g_p, y \rangle \leqslant \mathbf{E} \max_{x \in K} \langle g_n, x \rangle,$$

where g_n is a standard n-dimensional Gaussian vector.

The map $x \oplus y \mapsto x \otimes y$ is the contraction on $S^{d-1} \times S^{d-1}$,

$$|x \otimes y - x' \otimes y'| \leqslant \left(|x - x'|^2 + |y - y'|^2 \right)^{1/2}. \qquad (1)$$

The inequality (1) is false on $\mathbf{C}^d$, even for $d = 1$.

Problem

How to use a Slepian-type lemma for **complex** *Gaussian matrices ?*

Rectangular matrices

Let $X = \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$, equipped with operator norm. Dvoretzky's theorem controls the norm (largest singular value) on a large-dimensional subspace.

One can expect more : if $N \gg d$, a typical $N \times d$ Gaussian matrix G will be close to an isometry. Let $s_{\min}(G) = \min_{|x|=1} |Gx|$. We have by a net argument, that with large probability

$$\sqrt{N} - C\sqrt{d} \leqslant s_{\min}(G) \leqslant \|G\| \leqslant \sqrt{N} + C\sqrt{d}$$

We can use another net argument to prove the following :

Theorem

Fix $\varepsilon > 0$, and let $N \geqslant Cd/\varepsilon^2$. Let $E \subset X$ be a random d-dimensional subspace. Then with large probability, every matrix $A \in E$ satisfies

$$(1-\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}} \leqslant s_{min}(A) \leqslant \|A\|_{op} \leqslant (1+\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}}$$

Call such a subspace a **strong Dvoretzky subspace**. In the real case, Slepian-Gordon lemma leads to better estimates in the constants.

Rectangular matrices

Let $X = \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$, equipped with operator norm. Dvoretzky's theorem controls the norm (largest singular value) on a large-dimensional subspace. One can expect more : if $N \gg d$, a typical $N \times d$ Gaussian matrix G will be close to an isometry. Let $s_{\min}(G) = \min_{|x|=1} |Gx|$. We have by a net argument, that with large probability

$$\sqrt{N} - C\sqrt{d} \leqslant s_{\min}(G) \leqslant \|G\| \leqslant \sqrt{N} + C\sqrt{d}$$

We can use another net argument to prove the following :

Theorem

Fix $\varepsilon > 0$, and let $N \geqslant Cd/\varepsilon^2$. Let $E \subset X$ be a random d-dimensional subspace. Then with large probability, every matrix $A \in E$ satisfies

$$(1-\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}} \leqslant s_{min}(A) \leqslant \|A\|_{op} \leqslant (1+\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}}$$

Call such a subspace a **strong Dvoretzky subspace**. In the real case, Slepian-Gordon lemma leads to better estimates in the constants.

Rectangular matrices

Let $X = \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$, equipped with operator norm. Dvoretzky's theorem controls the norm (largest singular value) on a large-dimensional subspace. One can expect more : if $N \gg d$, a typical $N \times d$ Gaussian matrix G will be close to an isometry. Let $s_{\min}(G) = \min_{|x|=1} |Gx|$. We have by a net argument, that with large probability

$$\sqrt{N} - C\sqrt{d} \leqslant s_{\min}(G) \leqslant \|G\| \leqslant \sqrt{N} + C\sqrt{d}$$

We can use another net argument to prove the following :

Theorem

Fix $\varepsilon > 0$, and let $N \geqslant Cd/\varepsilon^2$. Let $E \subset X$ be a random d-dimensional subspace. Then with large probability, every matrix $A \in E$ satisfies

$$(1-\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}} \leqslant s_{min}(A) \leqslant \|A\|_{op} \leqslant (1+\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}}$$

Call such a subspace a **strong Dvoretzky subspace**. In the real case, Slepian-Gordon lemma leads to better estimates in the constants.

Rectangular matrices

Let $X = \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$, equipped with operator norm. Dvoretzky's theorem controls the norm (largest singular value) on a large-dimensional subspace. One can expect more : if $N \gg d$, a typical $N \times d$ Gaussian matrix G will be close to an isometry. Let $s_{\min}(G) = \min_{|x|=1} |Gx|$. We have by a net argument, that with large probability

$$\sqrt{N} - C\sqrt{d} \leqslant s_{\min}(G) \leqslant \|G\| \leqslant \sqrt{N} + C\sqrt{d}$$

We can use another net argument to prove the following :

Theorem

Fix $\varepsilon > 0$, and let $N \geqslant Cd/\varepsilon^2$. Let $E \subset X$ be a random d-dimensional subspace. Then with large probability, every matrix $A \in E$ satisfies

$$(1-\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}} \leqslant s_{min}(A) \leqslant \|A\|_{op} \leqslant (1+\varepsilon)\frac{\|A\|_{HS}}{\sqrt{d}}$$

Call such a subspace a **strong Dvoretzky subspace**. In the real case, Slepian-Gordon lemma leads to better estimates in the constants.

Correspondance between subspaces and completely positive maps

Let $\Phi : \mathbf{C}^d \to \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ and $\Phi_i : \mathbf{C}^d \to \mathbf{C}^d$ to be the i-th row of Φ.

$$\Phi(x) = \sum_{i=1}^{N} |e_i\rangle\langle\Phi_i(x)|$$

- We denote by $|a\rangle\langle b|$ the rank one operator $c \mapsto \langle b, c\rangle a$,
- $(|a\rangle\langle b|)^* = |b\rangle\langle a|$,
- $(|a\rangle\langle b|)(|c\rangle\langle d|) = \langle b, c\rangle |a\rangle\langle d|$.

$$\Psi(x) := \Phi(x)^*\Phi(x) = \sum_{i=1}^{N} |\Phi_i(x)\rangle\langle\Phi_i(x)| = \sum_{i=1}^{N} \Phi_i|x\rangle\langle x|\Phi_i^*$$

Identifying a unit vector x with $|x\rangle\langle x|$, Ψ can be defined on $\mathcal{M}(\mathbf{C}^d)$ as

$$\Psi(\rho) = \sum_{i=1}^{N} \Phi_i \rho \Phi_i^*.$$

Correspondance between subspaces and completely positive maps

Let $\Phi : \mathbf{C}^d \to \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ and $\Phi_i : \mathbf{C}^d \to \mathbf{C}^d$ to be the i-th row of Φ.

$$\Phi(x) = \sum_{i=1}^{N} |e_i\rangle\langle\Phi_i(x)|$$

$$\Psi(x) := \Phi(x)^*\Phi(x) = \sum_{i=1}^{N} |\Phi_i(x)\rangle\langle\Phi_i(x)| = \sum_{i=1}^{N} \Phi_i|x\rangle\langle x|\Phi_i^*$$

Identifying a unit vector x with $|x\rangle\langle x|$, Ψ can be defined on $\mathcal{M}(\mathbf{C}^d)$ as

$$\Psi(\rho) = \sum_{i=1}^{N} \Phi_i \rho \Phi_i^*.$$

$$(1-\varepsilon)^{1/2} \leqslant s_{\min}(A) \leqslant \|A\| \leqslant (1+\varepsilon)^{1/2} \iff \|A^*A - \mathrm{Id}\|_{op} \leqslant \varepsilon.$$

Therefore the range of Φ consists of (multiples of) almost isometries iff the range of Ψ consists of almost multiples of Id.

Correspondance between subspaces and completely positive maps

Let $\Phi : \mathbf{C}^d \to \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ and $\Phi_i : \mathbf{C}^d \to \mathbf{C}^d$ to be the i-th row of Φ.

$$\Phi(x) = \sum_{i=1}^{N} |e_i\rangle\langle\Phi_i(x)|$$

$$\Psi(x) := \Phi(x)^*\Phi(x) = \sum_{i=1}^{N} |\Phi_i(x)\rangle\langle\Phi_i(x)| = \sum_{i=1}^{N} \Phi_i|x\rangle\langle x|\Phi_i^*$$

Identifying a unit vector x with $|x\rangle\langle x|$, Ψ can be defined on $\mathcal{M}(\mathbf{C}^d)$ as

$$\Psi(\rho) = \sum_{i=1}^{N} \Phi_i\rho\Phi_i^*.$$

$$(1-\varepsilon)^{1/2} \leqslant s_{\min}(A) \leqslant \|A\| \leqslant (1+\varepsilon)^{1/2} \iff \|A^*A - \mathrm{Id}\|_{op} \leqslant \varepsilon.$$

Therefore the range of Φ consists of (multiples of) almost isometries iff the range of Ψ consists of almost multiples of Id.

Correspondance between subspaces and completely positive maps

Let $\Phi : \mathbf{C}^d \to \mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ and $\Phi_i : \mathbf{C}^d \to \mathbf{C}^d$ to be the i-th row of Φ.

$$\Phi(x) = \sum_{i=1}^{N} |e_i\rangle\langle\Phi_i(x)|$$

$$\Psi(x) := \Phi(x)^*\Phi(x) = \sum_{i=1}^{N} |\Phi_i(x)\rangle\langle\Phi_i(x)| = \sum_{i=1}^{N} \Phi_i|x\rangle\langle x|\Phi_i^*$$

Identifying a unit vector x with $|x\rangle\langle x|$, Ψ can be defined on $\mathcal{M}(\mathbf{C}^d)$ as

$$\Psi(\rho) = \sum_{i=1}^{N} \Phi_i \rho \Phi_i^*.$$

$$(1-\varepsilon)^{1/2} \leqslant s_{\min}(A) \leqslant \|A\| \leqslant (1+\varepsilon)^{1/2} \iff \|A^*A - \mathrm{Id}\|_{op} \leqslant \varepsilon.$$

Therefore the range of Φ consists of (multiples of) almost isometries iff the range of Ψ consists of almost multiples of Id.

Completely positive maps

Definition

A linear map $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is **completely positive** *(CP) if $\Phi \otimes \mathrm{Id}_{\mathcal{M}(\mathbf{C}^k)}$ maps positive matrices to positive matrices for any k. This is equivalent to say that there are matrices $V_i \in \mathcal{M}(\mathbf{C}^d)$ so that*

$$\Phi(X) = \sum_{i=1}^{N} V_i X V_i^* \qquad \text{(Kraus decomposition).}$$

The minimal such N is called the Kraus rank of Φ and is at most d^2.

Definition

A **state** *$\rho \in \mathcal{M}(\mathbf{C}^d)$ is a positive self-adjoint matrix with trace 1.*

- The set of states is the convex hull of rank one projectors $|x\rangle\langle x|$, which are called **pure states**.
- The state $\frac{\mathrm{Id}}{d}$ (the **maximally mixed state**) plays a central role.

Completely positive maps

Definition

A linear map $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is **completely positive** *(CP) if $\Phi \otimes \mathrm{Id}_{\mathcal{M}(\mathbf{C}^k)}$ maps positive matrices to positive matrices for any k. This is equivalent to say that there are matrices $V_i \in \mathcal{M}(\mathbf{C}^d)$ so that*

$$\Phi(X) = \sum_{i=1}^{N} V_i X V_i^* \qquad \text{(Kraus decomposition).}$$

The minimal such N is called the Kraus rank of Φ and is at most d^2.

Definition

A **state** *$\rho \in \mathcal{M}(\mathbf{C}^d)$ is a positive self-adjoint matrix with trace 1.*

- The set of states is the convex hull of rank one projectors $|x\rangle\langle x|$, which are called **pure states**.
- The state $\frac{\mathrm{Id}}{d}$ (the **maximally mixed state**) plays a central role.

Completely positive maps

Definition

A linear map $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is **completely positive** *(CP) if $\Phi \otimes \mathrm{Id}_{\mathcal{M}(\mathbf{C}^k)}$ maps positive matrices to positive matrices for any k. This is equivalent to say that there are matrices $V_i \in \mathcal{M}(\mathbf{C}^d)$ so that*

$$\Phi(X) = \sum_{i=1}^{N} V_i X V_i^* \qquad \text{(Kraus decomposition).}$$

The minimal such N is called the Kraus rank of Φ and is at most d^2.

Definition

A **state** *$\rho \in \mathcal{M}(\mathbf{C}^d)$ is a positive self-adjoint matrix with trace 1.*

- The set of states is the convex hull of rank one projectors $|x\rangle\langle x|$, which are called **pure states**.
- The state $\frac{\mathrm{Id}}{d}$ (the **maximally mixed state**) plays a central role.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr}\Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E} UXU^* = V(\mathbf{E} UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E} UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr}\Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E} UXU^* = V(\mathbf{E} UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E} UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr}\Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E} UXU^* = V(\mathbf{E} UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E} UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr}\Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E}UXU^* = V(\mathbf{E}UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E}UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr} \Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E} UXU^* = V(\mathbf{E} UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E} UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

Quantum channels

Definition

A **quantum channel** Φ *is a completely positive map which preseves trace*

$$\operatorname{Tr}\Phi(X) = \operatorname{Tr} X.$$

- A quantum channel maps states to states.
- If (U_i) are unitary matrices, then $X \mapsto \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^*$ is a quantum channel.
- The depolarizing channel $R : X \mapsto \mathbf{E} UXU^*$ with U Haar-distributed on the unitary group $\mathcal{U}(d)$.
- $R(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d}$.
  Proof : since $\mathbf{E} UXU^* = V(\mathbf{E} UXU^*)V^*$ for any $V \in \mathcal{U}(d)$, $\mathbf{E} UXU^*$ commutes to $\mathcal{M}(\mathbf{C}^d)$, so it is a multiple of identity.
- The Kraus rank of R is d^2.

ε-randomizing channels

Definition (Hayden, Leung, Shor and Winter)

For $0 < \varepsilon < 1$, a quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is ε-randomizing if for any state ρ

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_\infty \leqslant \frac{\varepsilon}{d} \tag{2}$$

i.e. the spectrum of $\Phi(\rho)$ belongs to $[\frac{1-\varepsilon}{d}, \frac{1+\varepsilon}{d}]$.

1. By a convexity argument, it is enough to check (2) on pure states.
2. Let $\Phi : X \mapsto \sum_{i=1}^N U_i X U_i^*$, and for $1 \leqslant j \leqslant d$, let A_j be the $N \times d$ matrix whose i-th row is the j-th column of U_i. Then Φ is ε-randomizing if and only if (A_j) span a strong Dvoretzky subspace

$$|\alpha|\sqrt{\frac{N}{d}}\sqrt{1-\varepsilon} \leqslant s_{\min}\left(\sum_{j=1}^d \alpha_j A_j\right) \leqslant \left\|\sum_{j=1}^d \alpha_j A_j\right\|_{op} \leqslant |\alpha|\sqrt{\frac{N}{d}}\sqrt{1+\varepsilon}$$

ε-randomizing channels

Definition (Hayden, Leung, Shor and Winter)

For $0 < \varepsilon < 1$, a quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is ε-randomizing if for any state ρ

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_\infty \leqslant \frac{\varepsilon}{d} \tag{2}$$

i.e. the spectrum of $\Phi(\rho)$ belongs to $[\frac{1-\varepsilon}{d}, \frac{1+\varepsilon}{d}]$.

1. By a convexity argument, it is enough to check (2) on pure states.
2. Let $\Phi : X \mapsto \sum_{i=1}^N U_i X U_i^*$, and for $1 \leqslant j \leqslant d$, let A_j be the $N \times d$ matrix whose i-th row is the j-th column of U_i. Then Φ is ε-randomizing if and only if (A_j) span a strong Dvoretzky subspace

$$|\alpha| \sqrt{\frac{N}{d}} \sqrt{1-\varepsilon} \leqslant s_{\min} \left(\sum_{j=1}^d \alpha_j A_j \right) \leqslant \left\| \sum_{j=1}^d \alpha_j A_j \right\|_{op} \leqslant |\alpha| \sqrt{\frac{N}{d}} \sqrt{1+\varepsilon}$$

ε-randomizing channels

Definition (Hayden, Leung, Shor and Winter)

For $0 < \varepsilon < 1$, a quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is ε-randomizing if for any state ρ

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_\infty \leqslant \frac{\varepsilon}{d} \qquad (2)$$

i.e. the spectrum of $\Phi(\rho)$ belongs to $[\frac{1-\varepsilon}{d}, \frac{1+\varepsilon}{d}]$.

1. By a convexity argument, it is enough to check (2) on pure states.
2. Let $\Phi : X \mapsto \sum_{i=1}^N U_i X U_i^*$, and for $1 \leqslant j \leqslant d$, let A_j be the $N \times d$ matrix whose i-th row is the j-th column of U_i. Then Φ is ε-randomizing if and only if (A_j) span a strong Dvoretzky subspace

$$|\alpha|\sqrt{\frac{N}{d}}\sqrt{1-\varepsilon} \leqslant s_{\min}\left(\sum_{j=1}^d \alpha_j A_j\right) \leqslant \left\|\sum_{j=1}^d \alpha_j A_j\right\|_{op} \leqslant |\alpha|\sqrt{\frac{N}{d}}\sqrt{1+\varepsilon}$$

- ε-randomizing channels are useful in quantum information theory, and especially quantum cryptography.
- The depolarizing channel is 0-randomizing, but has maximal Kraus rank, equal to d^2. Any Kraus decomposition of size d^2 yields a d-dimensional subspace of $\mathcal{M}(\mathbf{C}^N, \mathbf{C}^d)$ in which every matrix is a multiple of an isometry.

Problem

Find ε-randomizing channels with small Kraus rank (proportional to d). Even better, find explicitly such channels.

- A ε-randomizing channel must satisfy $N \geqslant d$.
  Elementary algebraic geometry shows that a subspace of $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ in which every nonzero matrix is invertible has dimension $\leqslant N - d + 1$, so the channel satisfies $N \geqslant 2d - 1$.
- Random channels will provide examples with N proportional to d (we could take $N = (2 + \eta)d$ in the real using Slepian-Gordon lemma).

- ε-randomizing channels are useful in quantum information theory, and especially quantum cryptography.
- The depolarizing channel is 0-randomizing, but has maximal Kraus rank, equal to d^2. Any Kraus decomposition of size d^2 yields a d-dimensional subspace of $\mathcal{M}(\mathbf{C}^N, \mathbf{C}^d)$ in which every matrix is a multiple of an isometry.

Problem

Find ε-randomizing channels with small Kraus rank (proportional to d). Even better, find explicitly such channels.

- A ε-randomizing channel must satisfy $N \geqslant d$. Elementary algebraic geometry shows that a subspace of $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ in which every nonzero matrix is invertible has dimension $\leqslant N - d + 1$, so the channel satisfies $N \geqslant 2d - 1$.
- Random channels will provide examples with N proportional to d (we could take $N = (2 + \eta)d$ in the real using Slepian-Gordon lemma).

- ε-randomizing channels are useful in quantum information theory, and especially quantum cryptography.
- The depolarizing channel is 0-randomizing, but has maximal Kraus rank, equal to d^2. Any Kraus decomposition of size d^2 yields a d-dimensional subspace of $\mathcal{M}(\mathbf{C}^N, \mathbf{C}^d)$ in which every matrix is a multiple of an isometry.

Problem

Find ε-randomizing channels with small Kraus rank (proportional to d). Even better, find explicitly such channels.

- A ε-randomizing channel must satisfy $N \geqslant d$. Elementary algebraic geometry shows that a subspace of $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ in which every nonzero matrix is invertible has dimension $\leqslant N - d + 1$, so the channel satisfies $N \geqslant 2d - 1$.
- Random channels will provide examples with N proportional to d (we could take $N = (2 + \eta)d$ in the real using Slepian-Gordon lemma).

- ε-randomizing channels are useful in quantum information theory, and especially quantum cryptography.
- The depolarizing channel is 0-randomizing, but has maximal Kraus rank, equal to d^2. Any Kraus decomposition of size d^2 yields a d-dimensional subspace of $\mathcal{M}(\mathbf{C}^N, \mathbf{C}^d)$ in which every matrix is a multiple of an isometry.

Problem

Find ε-randomizing channels with small Kraus rank (proportional to d). Even better, find explicitly such channels.

- A ε-randomizing channel must satisfy $N \geqslant d$.
  Elementary algebraic geometry shows that a subspace of $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ in which every nonzero matrix is invertible has dimension $\leqslant N - d + 1$, so the channel satisfies $N \geqslant 2d - 1$.
- Random channels will provide examples with N proportional to d (we could take $N = (2 + \eta)d$ in the real using Slepian-Gordon lemma).

- ε-randomizing channels are useful in quantum information theory, and especially quantum cryptography.
- The depolarizing channel is 0-randomizing, but has maximal Kraus rank, equal to d^2. Any Kraus decomposition of size d^2 yields a d-dimensional subspace of $\mathcal{M}(\mathbf{C}^N, \mathbf{C}^d)$ in which every matrix is a multiple of an isometry.

Problem

Find ε-randomizing channels with small Kraus rank (proportional to d). Even better, find explicitly such channels.

- A ε-randomizing channel must satisfy $N \geqslant d$.
  Elementary algebraic geometry shows that a subspace of $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$ in which every nonzero matrix is invertible has dimension $\leqslant N - d + 1$, so the channel satisfies $N \geqslant 2d - 1$.
- Random channels will provide examples with N proportional to d (we could take $N = (2 + \eta)d$ in the real using Slepian-Gordon lemma).

Short ε-randomizing channels

Theorem (Hayden, Leung, Shor, Winter — A.)

Let $U_1, \ldots, U_N$ be i.i.d. Haar-distributed random $d \times d$ unitary matrices. Then for $N \geqslant Cd/\varepsilon^2$, the quantum channel

$$\Phi : X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$$

is ε-randomizing with exponentially large probability.

- HLSW had the weaker estimate $N \geqslant Cd \log d/\varepsilon^2$.
- Optimal dependence in d.
- For such random constructions, the dependence in ε is optimal.

Question

Are there ε-randomizing channels with a better dependence in ε ?

Short ε-randomizing channels

Theorem (Hayden, Leung, Shor, Winter — A.)

Let $U_1, \ldots, U_N$ be i.i.d. Haar-distributed random $d \times d$ unitary matrices. Then for $N \geqslant Cd/\varepsilon^2$, the quantum channel

$$\Phi : X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$$

is ε-randomizing with exponentially large probability.

- HLSW had the weaker estimate $N \geqslant Cd \log d/\varepsilon^2$.
- Optimal dependence in d.
- For such random constructions, the dependence in ε is optimal.

Question

Are there ε-randomizing channels with a better dependence in ε ?

Short ε-randomizing channels

Theorem (Hayden, Leung, Shor, Winter — A.)

Let $U_1, \ldots, U_N$ be i.i.d. Haar-distributed random $d \times d$ unitary matrices. Then for $N \geqslant Cd/\varepsilon^2$, the quantum channel

$$\Phi : X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$$

is ε-randomizing with exponentially large probability.

- HLSW had the weaker estimate $N \geqslant Cd \log d/\varepsilon^2$.
- Optimal dependence in d.
- For such random constructions, the dependence in ε is optimal.

Question

Are there ε-randomizing channels with a better dependence in ε ?

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then

$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\operatorname{Tr} \sigma \Delta(\rho)| := B$$

3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\operatorname{Tr} \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$

   Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then

$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\mathrm{Tr}\, \sigma \Delta(\rho)| := B$$

3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\mathrm{Tr}\, \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$

   Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then

$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\,\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\,\mathrm{Tr}\, \sigma \Delta(\rho)| := B$$

3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\mathrm{Tr}\, \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$

   Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then

$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\operatorname{Tr} \sigma \Delta(\rho)| := B$$

   Proof : For every pure states ρ, σ, there are $\rho_0, \sigma_0 \in \mathcal{N}$ so that $\|\rho - \rho_0\|_1 \leqslant \delta$, $\|\sigma - \sigma_0\| \leqslant \delta$. Then

$$|\operatorname{Tr} \sigma \Delta(\rho)| \leqslant |\operatorname{Tr} (\sigma - \sigma_0) \Delta(\rho)| + |\operatorname{Tr} \sigma_0 \Delta(\rho - \rho_0)| + |\operatorname{Tr} \sigma_0 \Delta(\rho_0)|$$

   Taking supremum over ρ, σ gives $A \leqslant \delta A + \delta A + B$.
3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\operatorname{Tr} \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N}\sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then
$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\,\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\,\mathrm{Tr}\, \sigma \Delta(\rho)| := B$$
3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\mathrm{Tr}\, \sigma \Delta(\rho) = \frac{1}{N}\sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$

   Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then
$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\mathrm{Tr}\, \sigma \Delta(\rho)| := B$$
3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\mathrm{Tr}\, \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$
Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then

$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\operatorname{Tr} \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\operatorname{Tr} \sigma \Delta(\rho)| := B$$

3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\operatorname{Tr} \sigma \Delta(\rho) = \dfrac{1}{N} \displaystyle\sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \dfrac{1}{d}$
   Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Proof of the theorem

Let $\Phi : \rho \mapsto \frac{1}{N} \sum U_i \rho U_i^*$, $R : \rho \mapsto \frac{\mathrm{Id}}{d}$ and $\Delta = \Phi - R$. Let $\mathcal{S}$ be the set of states ; we need to show that for any $\rho \in \mathcal{S}$, $\|\Delta(\rho)\|_{op} \leqslant \frac{\varepsilon}{d}$, i.e.

$$\sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{\varepsilon}{d}.$$

1. We can restrict the supremum to pure states
2. Let $\mathcal{N}$ be a δ-net (w.r.t. $\|\cdot\|_1$) in the set of pure states. Then
$$A := \sup_{\rho,\sigma \in \mathcal{S}} |\mathrm{Tr}\, \sigma \Delta(\rho)| \leqslant \frac{1}{1-2\delta} \sup_{\rho,\sigma \in \mathcal{N}} |\mathrm{Tr}\, \sigma \Delta(\rho)| := B$$
3. For fixed $\rho = |x\rangle\langle x|, \sigma = |y\rangle\langle y|$, $\mathrm{Tr}\, \sigma \Delta(\rho) = \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y\rangle|^2 - \frac{1}{d}$
Using Bernstein inequalities, this quantity is smaller that ε/d with probability $1 - 2\exp(-cN\varepsilon^2)$
4. There is a $1/4$-net in the set of pure states of cardinality 400^d.
5. The union bound work for $cN\varepsilon^2 \geqslant d \log 400 + \log 2$.

Derandomization

The same net argument works for i.i.d. copies of a $\mathcal{U}(d)$-valued random vector U which is

1. **isotropic** : for any unit vectors $x, y \in \mathbf{C}^d$, $\mathbf{E}|\langle Ux, y\rangle|^2 = \frac{1}{d}$. This is equivalent to say that the covariance matrix of U is the same as the Haar distribution.
2. **subgaussian** : for any $x, y \in \mathbf{C}^d$, if $Z = \langle Ux, y\rangle$,

$$\mathbf{P}(|Z| \geqslant t(\mathbf{E}|Z|^2)^{1/2}) \leqslant C \exp(-ct^2).$$

Any subgaussian random vector has exponentially large support (already in $\mathbf{C}^d$), so this proof cannot go below $N \times Cd \approx d^2$ random bits.

Question (Hayden–Leung–Shor–Winter)

Can we drop the hypothesis "U subgaussian" ?

Derandomization

The same net argument works for i.i.d. copies of a $\mathcal{U}(d)$-valued random vector U which is

1. **isotropic** : for any unit vectors $x, y \in \mathbf{C}^d$, $\mathbf{E}|\langle Ux, y\rangle|^2 = \frac{1}{d}$. This is equivalent to say that the covariance matrix of U is the same as the Haar distribution.
2. **subgaussian** : for any $x, y \in \mathbf{C}^d$, if $Z = \langle Ux, y\rangle$,

$$\mathbf{P}(|Z| \geqslant t(\mathbf{E}|Z|^2)^{1/2}) \leqslant C \exp(-ct^2).$$

Any subgaussian random vector has exponentially large support (already in $\mathbf{C}^d$), so this proof cannot go below $N \times Cd \approx d^2$ random bits.

Question (Hayden–Leung–Shor–Winter)

Can we drop the hypothesis "U subgaussian" ?

Derandomization

The same net argument works for i.i.d. copies of a $\mathcal{U}(d)$-valued random vector U which is

1. **isotropic** : for any unit vectors $x, y \in \mathbf{C}^d$, $\mathbf{E}|\langle Ux, y\rangle|^2 = \frac{1}{d}$. This is equivalent to say that the covariance matrix of U is the same as the Haar distribution.
2. **subgaussian** : for any $x, y \in \mathbf{C}^d$, if $Z = \langle Ux, y\rangle$,

$$\mathbf{P}(|Z| \geqslant t(\mathbf{E}|Z|^2)^{1/2}) \leqslant C \exp(-ct^2).$$

Any subgaussian random vector has exponentially large support (already in $\mathbf{C}^d$), so this proof cannot go below $N \times Cd \approx d^2$ random bits.

Question (Hayden–Leung–Shor–Winter)

Can we drop the hypothesis "U subgaussian" ?

Non-subgaussian isotropic $\mathcal{U}(d)$-valued vectors

Consider the Pauli matrices

$$\sigma_0 = \mathrm{Id}_2, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Then for any $X \in \mathcal{M}_2(\mathbf{C})$,

$$\frac{1}{4}\left(\sigma_0 X \sigma_0^* + \sigma_1 X \sigma_1^* + \sigma_2 X \sigma_2^* + \sigma_3 X \sigma_3^*\right) = \operatorname{Tr} X \frac{\mathrm{Id}}{2}.$$

  so the uniform measure on $\{\sigma_i\}$ is isotropic.
- Similarly, for any k, the uniform measure on k-fold tensor product of Pauli matrices is isotropic in $\mathcal{M}(\mathbf{C}^{2^k})$.
- Replacing random Haar matrices by Pauli matrices would also give ε-randomizing channels with extra tensor structure.

Non-subgaussian isotropic $\mathcal{U}(d)$-valued vectors

Consider the Pauli matrices

$$\sigma_0 = \mathrm{Id}_2, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Then for any $X \in \mathcal{M}_2(\mathbf{C})$,

$$\frac{1}{4}\left(\sigma_0 X \sigma_0^* + \sigma_1 X \sigma_1^* + \sigma_2 X \sigma_2^* + \sigma_3 X \sigma_3^*\right) = \operatorname{Tr} X \frac{\mathrm{Id}}{2}.$$

  so the uniform measure on $\{\sigma_i\}$ is isotropic.
- Similarly, for any k, the uniform measure on k-fold tensor product of Pauli matrices is isotropic in $\mathcal{M}(\mathbf{C}^{2^k})$.
- Replacing random Haar matrices by Pauli matrices would also give ε-randomizing channels with extra tensor structure.

Non-subgaussian isotropic $\mathcal{U}(d)$-valued vectors

Consider the Pauli matrices

$$\sigma_0 = \mathrm{Id}_2, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Then for any $X \in \mathcal{M}_2(\mathbf{C})$,

$$\frac{1}{4}\left(\sigma_0 X \sigma_0^* + \sigma_1 X \sigma_1^* + \sigma_2 X \sigma_2^* + \sigma_3 X \sigma_3^*\right) = \operatorname{Tr} X \frac{\mathrm{Id}}{2}.$$

  so the uniform measure on $\{\sigma_i\}$ is isotropic.
- Similarly, for any k, the uniform measure on k-fold tensor product of Pauli matrices is isotropic in $\mathcal{M}(\mathbf{C}^{2^k})$.
- Replacing random Haar matrices by Pauli matrices would also give ε-randomizing channels with extra tensor structure.

General isotropic vectors

Question (Hayden–Leung–Shor–Winter)

Can we construct a ε-randomizing channel from Cd/ε^2 i.i.d. copies of any isotropic $\mathcal{U}(d)$-valued random vector ?

- No ; it can be checked that one needs $N \geqslant C(\varepsilon) d \log d$ in some cases. Related to the *coupon's collector problem*.
- Yes if we allow extra logarithmic factors.

Theorem (A.)

If U is a $\mathcal{U}(d)$-valued isotropic random vector and U_i denote i.i.d. copies, is the channel

$$X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$$

is ε-randomizing with nonzero probability when $N \geqslant Cd \log^6 d/\varepsilon^2$.

General isotropic vectors

Question (Hayden–Leung–Shor–Winter)

Can we construct a ε-randomizing channel from Cd/ε^2 i.i.d. copies of any isotropic $\mathcal{U}(d)$-valued random vector ?

- No ; it can be checked that one needs $N \geqslant C(\varepsilon) d \log d$ in some cases. Related to the *coupon's collector problem*.
- Yes if we allow extra logarithmic factors.

Theorem (A.)

If U is a $\mathcal{U}(d)$-valued isotropic random vector and U_i denote i.i.d. copies, is the channel

$$X \mapsto \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^*$$

is ε-randomizing with nonzero probability when $N \geqslant Cd \log^6 d/\varepsilon^2$.

Proof (1)

We need to estimate, for $U_i \in \mathcal{U}(d)$ i.i.d. isotropic

$$\begin{aligned} M &= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y \rangle|^2 - \frac{1}{d} \right| \\ &= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^{N} |\operatorname{Tr} U_i |x\rangle\langle y||^2 - \frac{1}{d} \right| \\ &\leqslant \mathbf{E} \sup_{A \in B(S_1^d)} \left| \frac{1}{N} \sum_{i=1}^{N} |\operatorname{Tr} U_i A|^2 - \mathbf{E} \operatorname{Tr} |UA|^2 \right| \end{aligned}$$

This is an empirical process in the Schatten space $S_1^d = (\mathcal{M}(\mathbf{C}^d), \| \cdot \|_1)$.

$$B(S_1^d) = \operatorname{conv} \{ |x\rangle\langle y|, x, y \in \mathbf{C}^d, |x| = |y| = 1 \}.$$

Proof (1)

We need to estimate, for $U_i \in \mathcal{U}(d)$ i.i.d. isotropic

$$\begin{aligned} M &= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^N |\langle U_i x, y\rangle|^2 - \frac{1}{d} \right| \\ &= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^N |\operatorname{Tr} U_i |x\rangle\langle y||^2 - \frac{1}{d} \right| \\ &\leqslant \mathbf{E} \sup_{A \in B(S_1^d)} \left| \frac{1}{N} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2 - \mathbf{E} \operatorname{Tr} |UA|^2 \right| \end{aligned}$$

This is an empirical process in the Schatten space $S_1^d = (\mathcal{M}(\mathbf{C}^d), \|\cdot\|_1)$.

$$B(S_1^d) = \operatorname{conv} \{|x\rangle\langle y|, x, y \in \mathbf{C}^d, |x| = |y| = 1\}.$$

Proof (1)

We need to estimate, for $U_i \in \mathcal{U}(d)$ i.i.d. isotropic

$$
\begin{aligned}
M &= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^{N} |\langle U_i x, y \rangle|^2 - \frac{1}{d} \right| \\
&= \mathbf{E} \sup_{|x|=|y|=1} \left| \frac{1}{N} \sum_{i=1}^{N} |\operatorname{Tr} U_i |x\rangle\langle y||^2 - \frac{1}{d} \right| \\
&\leqslant \mathbf{E} \sup_{A \in B(S_1^d)} \left| \frac{1}{N} \sum_{i=1}^{N} |\operatorname{Tr} U_i A|^2 - \mathbf{E} \operatorname{Tr} |UA|^2 \right|
\end{aligned}
$$

This is an empirical process in the Schatten space $S_1^d = (\mathcal{M}(\mathbf{C}^d), \|\cdot\|_1)$.

$$
B(S_1^d) = \operatorname{conv} \{ |x\rangle\langle y|, x, y \in \mathbf{C}^d, |x| = |y| = 1 \}.
$$

Proof (2)

We can use results by Rudelson and Guédon, Mendelson, Pajor, Tomczak-Jaegermann about empirical processes in a Banach space with a good modulus of convexity (such as Hilbert space, ℓ_1^d, S_1^d).

Proof (following [R],[GMPT])

- Symmetrization arguement à la Giné–Zinn

$$M \leqslant 2\mathbf{E}_U \mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \mathbf{E} \left| \frac{1}{N} \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right|$$

- The theorem follows from the next lemma

Lemma

Let $U_1, \dots, U_N \in \mathcal{U}(d)$ be **deterministic**, *$N \geqslant d$. Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Proof (2)

We can use results by Rudelson and Guédon, Mendelson, Pajor, Tomczak-Jaegermann about empirical processes in a Banach space with a good modulus of convexity (such as Hilbert space, ℓ_1^d, S_1^d).

Proof (following [R],[GMPT])

- Symmetrization arguement à la Giné–Zinn

$$M \leqslant 2\mathbf{E}_U \mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \mathbf{E} \left| \frac{1}{N} \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right|$$

- The theorem follows from the next lemma

Lemma

Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ be **deterministic**, *$N \geqslant d$. Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Proof (2)

We can use results by Rudelson and Guédon, Mendelson, Pajor, Tomczak-Jaegermann about empirical processes in a Banach space with a good modulus of convexity (such as Hilbert space, ℓ_1^d, S_1^d).

Proof (following [R],[GMPT])

- Symmetrization arguement à la Giné–Zinn

$$M \leqslant 2\mathbf{E}_U \mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \mathbf{E} \left| \frac{1}{N} \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right|$$

- The theorem follows from the next lemma

Lemma

Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ be **deterministic**, *$N \geqslant d$. Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Proof of the lemma

Lemma

Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ *be* **deterministic**, $N \geqslant d$. *Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Let (g_i) be independent $N(0,1)$

$$\begin{aligned} \mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| &\leqslant \sqrt{\frac{\pi}{2}} \mathbf{E}_g \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N g_i |\operatorname{Tr} U_i A|^2 \right| \\ &\leqslant C \int_0^\infty \sqrt{\log N(B(S_1^d), \delta, \varepsilon)} d\varepsilon \end{aligned}$$

Here δ the distance induced by the Gaussian process and $N(K, \delta, \varepsilon)$ the number of balls of radius ε in the metric δ needed to cover K.

Proof of the lemma

Lemma

Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ be **deterministic**, $N \geqslant d$. *Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Let (g_i) be independent $N(0,1)$

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant \sqrt{\frac{\pi}{2}} \mathbf{E}_g \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N g_i |\operatorname{Tr} U_i A|^2 \right|$$

$$\leqslant C \int_0^\infty \sqrt{\log N(B(S_1^d), \delta, \varepsilon)} d\varepsilon$$

Here δ the distance induced by the Gaussian process and $N(K, \delta, \varepsilon)$ the number of balls of radius ε in the metric δ needed to cover K.

Proof of the lemma

Lemma

Let $U_1, \ldots, U_N \in \mathcal{U}(d)$ be **deterministic**, $N \geqslant d$. *Then,*

$$\mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| \leqslant C \log^3 N \sqrt{\sup_{A \in B(S_1^d)} \sum_{i=1}^N |\operatorname{Tr} U_i A|^2}.$$

Let (g_i) be independent $N(0,1)$

$$\begin{aligned} \mathbf{E}_\varepsilon \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N \varepsilon_i |\operatorname{Tr} U_i A|^2 \right| &\leqslant \sqrt{\frac{\pi}{2}} \mathbf{E}_g \sup_{A \in B(S_1^d)} \left| \sum_{i=1}^N g_i |\operatorname{Tr} U_i A|^2 \right| \\ &\leqslant C \int_0^\infty \sqrt{\log N(B(S_1^d), \delta, \varepsilon)} d\varepsilon \end{aligned}$$

Here δ the distance induced by the Gaussian process and $N(K, \delta, \varepsilon)$ the number of balls of radius ε in the metric δ needed to cover K.

Proof of the lemma

The metric δ can be upper-bounded

$$\begin{aligned}\delta(A,B)^2 &= \sum_{i=1}^{N} \left| |\operatorname{Tr} U_i A|^2 - |\operatorname{Tr} U_i B|^2 \right|^2 \\ &\leqslant \left(\sum_{i=1}^{N} |\operatorname{Tr} U_i (A+B)|^2 \right) \left(\sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i (A-B)|^2 \right).\end{aligned}$$

This leads to the bound

$$\mathbf{E}_{\varepsilon} \cdots \leqslant C \left(\sup_{A \in B(S_1^d)} \sum_{i=1}^{N} |\operatorname{Tr} U_i A|^2 \right)^{1/2} \int_0^{\infty} \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon$$

with $|||A||| = \sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i A| \leqslant \|A\|_1$.

The unit ball L of $||| \cdot |||$ has N « faces » and contains $B(S_1^d)$.

Proof of the lemma

The metric δ can be upper-bounded

$$\begin{aligned} \delta(A,B)^2 &= \sum_{i=1}^{N} \left| |\operatorname{Tr} U_i A|^2 - |\operatorname{Tr} U_i B|^2 \right|^2 \\ &\leqslant \left(\sum_{i=1}^{N} |\operatorname{Tr} U_i (A+B)|^2 \right) \left(\sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i (A-B)|^2 \right). \end{aligned}$$

This leads to the bound

$$\mathbf{E}_\varepsilon \cdots \leqslant C \left(\sup_{A \in B(S_1^d)} \sum_{i=1}^{N} |\operatorname{Tr} U_i A|^2 \right)^{1/2} \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon$$

with $|||A||| = \sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i A| \leqslant \|A\|_1$.

The unit ball L of $||| \cdot |||$ has N « faces » and contains $B(S_1^d)$.

Proof of the lemma

The metric δ can be upper-bounded

$$\begin{aligned}\delta(A,B)^2 &= \sum_{i=1}^{N} \left| |\operatorname{Tr} U_i A|^2 - |\operatorname{Tr} U_i B|^2 \right|^2 \\ &\leqslant \left(\sum_{i=1}^{N} |\operatorname{Tr} U_i (A+B)|^2 \right) \left(\sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i (A-B)|^2 \right).\end{aligned}$$

This leads to the bound

$$\mathbf{E}_\varepsilon \cdots \leqslant C \left(\sup_{A \in B(S_1^d)} \sum_{i=1}^{N} |\operatorname{Tr} U_i A|^2 \right)^{1/2} \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon$$

with $|||A||| = \sup_{1 \leqslant i \leqslant N} |\operatorname{Tr} U_i A| \leqslant \|A\|_1$.

The unit ball L of $||| \cdot |||$ has N « faces » and contains $B(S_1^d)$.

Covering numbers

We need to estimate

$$I = \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon \overset{?}{\leqslant} C \log^3 N$$

Assume for the moment the duality property for covering numbers holds (it is still a conjecture)

$$\log N(K, L, \varepsilon) \leqslant C \log N(L^\circ, K^\circ, c\varepsilon)$$

This leads to

$$I \leqslant C \int_0^\infty \sqrt{\log N(L^\circ, B(S_\infty^d), \varepsilon)} d\varepsilon.$$

With L° the unit ball for $||| \cdot |||^*$ — a convex body with N « vertices » contained in $B(S_\infty^d)$.

Covering numbers

We need to estimate

$$I = \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon \overset{?}{\leqslant} C \log^3 N$$

Assume for the moment the duality property for covering numbers holds (it is still a conjecture)

$$\log N(K, L, \varepsilon) \leqslant C \log N(L^\circ, K^\circ, c\varepsilon)$$

This leads to

$$I \leqslant C \int_0^\infty \sqrt{\log N(L^\circ, B(S_\infty^d), \varepsilon)} d\varepsilon.$$

With L° the unit ball for $|||\cdot|||^*$ — a convex body with N « vertices » contained in $B(S_\infty^d)$.

Covering numbers

We need to estimate

$$I = \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon \overset{?}{\leqslant} C \log^3 N$$

Assume for the moment the duality property for covering numbers holds (it is still a conjecture)

$$\log N(K, L, \varepsilon) \leqslant C \log N(L^\circ, K^\circ, c\varepsilon)$$

This leads to

$$I \leqslant C \int_0^\infty \sqrt{\log N(L^\circ, B(S_\infty^d), \varepsilon)} d\varepsilon.$$

With L° the unit ball for $|||\cdot|||^*$ — a convex body with N « vertices » contained in $B(S_\infty^d)$.

Covering numbers

We need to estimate

$$I = \int_0^\infty \sqrt{\log N(B(S_1^d), |||.|||, \varepsilon)} d\varepsilon \overset{?}{\leqslant} C \log^3 N$$

Assume for the moment the duality property for covering numbers holds (it is still a conjecture)

$$\log N(K, L, \varepsilon) \leqslant C \log N(L^\circ, K^\circ, c\varepsilon)$$

This leads to

$$I \leqslant C \int_0^\infty \sqrt{\log N(L^\circ, B(S_\infty^d), \varepsilon)} d\varepsilon.$$

With L° the unit ball for $|||\cdot|||^*$ — a convex body with N « vertices » contained in $B(S_\infty^d)$.

End of the proof

Lemma (Maurey's lemma)

If $K \subset L$ and K has N « vertices », then for all $\varepsilon > 0$,

$$\varepsilon \sqrt{\log N(K, L, \varepsilon)} \leqslant C T_2(L) \sqrt{\log N}$$

Here $T_2(L)$ is the type 2 constant of the norm associated to L.

1. In our case $T_2(S_\infty^d) \leqslant C\sqrt{\log d}$ (Tomczak-Jaegermann).
2. The duality conjecture holds up to a logarithmic factor. This follows from results by Bourgain, Pajor, Szarek and Tomczak–Jaegermann since S_1^d has a equivalent norm which has a good modulus of convexity, namely the norm of S_p^d for $p = 1 + 1/\log d$ (Tomczak-Jaegermann, Ball–Carlen–Lieb).
3. Collect all the logarithms.

End of the proof

Lemma (Maurey's lemma)

If $K \subset L$ and K has N « vertices », then for all $\varepsilon > 0$,

$$\varepsilon \sqrt{\log N(K, L, \varepsilon)} \leqslant C T_2(L) \sqrt{\log N}$$

Here $T_2(L)$ is the type 2 constant of the norm associated to L.

1. In our case $T_2(S_\infty^d) \leqslant C\sqrt{\log d}$ (Tomczak-Jaegermann).
2. The duality conjecture holds up to a logarithmic factor. This follows from results by Bourgain, Pajor, Szarek and Tomczak–Jaegermann since S_1^d has a equivalent norm which has a good modulus of convexity, namely the norm of S_p^d for $p = 1 + 1/\log d$ (Tomczak-Jaegermann, Ball–Carlen–Lieb).
3. Collect all the logarithms.

End of the proof

Lemma (Maurey's lemma)

If $K \subset L$ and K has N « vertices », then for all $\varepsilon > 0$,

$$\varepsilon \sqrt{\log N(K, L, \varepsilon)} \leqslant C T_2(L) \sqrt{\log N}$$

Here $T_2(L)$ is the type 2 constant of the norm associated to L.

1. In our case $T_2(S_\infty^d) \leqslant C\sqrt{\log d}$ (Tomczak-Jaegermann).
2. The duality conjecture holds up to a logarithmic factor. This follows from results by Bourgain, Pajor, Szarek and Tomczak–Jaegermann since S_1^d has a equivalent norm which has a good modulus of convexity, namely the norm of S_p^d for $p = 1 + 1/\log d$ (Tomczak-Jaegermann, Ball–Carlen–Lieb).
3. Collect all the logarithms.

End of the proof

Lemma (Maurey's lemma)

If $K \subset L$ and K has N « vertices », then for all $\varepsilon > 0$,

$$\varepsilon\sqrt{\log N(K,L,\varepsilon)} \leqslant CT_2(L)\sqrt{\log N}$$

Here $T_2(L)$ is the type 2 constant of the norm associated to L.

1. In our case $T_2(S_\infty^d) \leqslant C\sqrt{\log d}$ (Tomczak-Jaegermann).
2. The duality conjecture holds up to a logarithmic factor. This follows from results by Bourgain, Pajor, Szarek and Tomczak–Jaegermann since S_1^d has a equivalent norm which has a good modulus of convexity, namely the norm of S_p^d for $p = 1 + 1/\log d$ (Tomczak-Jaegermann, Ball–Carlen–Lieb).
3. Collect all the logarithms.

Weakly ε-randomizing channels

A quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is weakly ε-randomizing if for any staty ρ,

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_{HS} \leqslant \frac{\varepsilon}{\sqrt{d}}$$

- Since $\| \cdot \|_{HS} \leqslant \sqrt{d} \| \cdot \|_{op}$, a ε-randomizing channel is weakly ε-randomizing.
- The Hilbert–Schmidt norm is easier to handle than the operator norm because it allows to use spectral methods.
- There are explicit examples of weakly ε-randomizing channels with Kraus rank less than $16d/\varepsilon^2$, using Pauli matrices (Ambainis—Smith, Dickinson—Nayak). Constructions are based on standard derandomisation techniques (small bias subsets of $(\mathbf{Z}/2\mathbf{Z})^N$).
- It seems hard to decide whether these channels are ε-randomizing in the strong sense.

Weakly ε-randomizing channels

A quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is weakly ε-randomizing if for any staty ρ,

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_{HS} \leqslant \frac{\varepsilon}{\sqrt{d}}$$

- Since $\| \cdot \|_{HS} \leqslant \sqrt{d} \| \cdot \|_{op}$, a ε-randomizing channel is weakly ε-randomizing.
- The Hilbert–Schmidt norm is easier to handle than the operator norm because it allows to use spectral methods.
- There are explicit examples of weakly ε-randomizing channels with Kraus rank less than $16d/\varepsilon^2$, using Pauli matrices (Ambainis—Smith, Dickinson—Nayak). Constructions are based on standard derandomisation techniques (small bias subsets of $(\mathbf{Z}/2\mathbf{Z})^N$).
- It seems hard to decide whether these channels are ε-randomizing in the strong sense.

Weakly ε-randomizing channels

A quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is weakly ε-randomizing if for any staty ρ,

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_{HS} \leqslant \frac{\varepsilon}{\sqrt{d}}$$

- Since $\|\cdot\|_{HS} \leqslant \sqrt{d}\|\cdot\|_{op}$, a ε-randomizing channel is weakly ε-randomizing.
- The Hilbert–Schmidt norm is easier to handle than the operator norm because it allows to use spectral methods.
- There are explicit examples of weakly ε-randomizing channels with Kraus rank less than $16d/\varepsilon^2$, using Pauli matrices (Ambainis—Smith, Dickinson—Nayak). Constructions are based on standard derandomisation techniques (small bias subsets of $(\mathbf{Z}/2\mathbf{Z})^N$).
- It seems hard to decide whether these channels are ε-randomizing in the strong sense.

Weakly ε-randomizing channels

A quantum channel $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is weakly ε-randomizing if for any staty ρ,

$$\left\| \Phi(\rho) - \frac{\mathrm{Id}}{d} \right\|_{HS} \leqslant \frac{\varepsilon}{\sqrt{d}}$$

- Since $\| \cdot \|_{HS} \leqslant \sqrt{d} \| \cdot \|_{op}$, a ε-randomizing channel is weakly ε-randomizing.
- The Hilbert–Schmidt norm is easier to handle than the operator norm because it allows to use spectral methods.
- There are explicit examples of weakly ε-randomizing channels with Kraus rank less than $16d/\varepsilon^2$, using Pauli matrices (Ambainis—Smith, Dickinson—Nayak). Constructions are based on standard derandomisation techniques (small bias subsets of $(\mathbf{Z}/2\mathbf{Z})^N$).
- It seems hard to decide whether these channels are ε-randomizing in the strong sense.

Additivity conjectures

Definition

The (von Neumann) **entropy** *of a state* ρ *is* $S(\rho) = -\operatorname{Tr} \rho \log \rho$.
The **minimal output entropy** *of a channel* Φ *is* $S_{\min}(\Phi) = \min_{\rho \in S} S(\Phi(\rho))$

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ *and* Ψ *are quantum channels, is it true thar*
$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$.

This would be implied (taking $p \to 1$) by the following

$$\max_{\rho} \|(\Phi \otimes \Psi)(\rho)\|_p = \max_{\rho} \|\Phi(\rho)\|_p \max_{\rho} \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$.

Additivity conjectures

Definition

The (von Neumann) **entropy** *of a state* ρ *is* $S(\rho) = -\operatorname{Tr} \rho \log \rho$.
The **minimal output entropy** *of a channel* Φ *is* $S_{\min}(\Phi) = \min_{\rho \in S} S(\Phi(\rho))$

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ *and* Ψ *are quantum channels, is it true thar*
$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$.

This would be implied (taking $p \to 1$) by the following

$$\max_{\rho} \|(\Phi \otimes \Psi)(\rho)\|_p = \max_{\rho} \|\Phi(\rho)\|_p \max_{\rho} \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$

Additivity conjectures

Definition

The (von Neumann) **entropy** *of a state* ρ *is* $S(\rho) = -\operatorname{Tr} \rho \log \rho$*.*
The **minimal output entropy** *of a channel* Φ *is* $S_{\min}(\Phi) = \min_{\rho \in S} S(\Phi(\rho))$

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ *and* Ψ *are quantum channels, is it true thar*
$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$*.*

This would be implied (taking $p \to 1$) by the following

$$\max_{\rho} \|(\Phi \otimes \Psi)(\rho)\|_p = \max_{\rho} \|\Phi(\rho)\|_p \max_{\rho} \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$

Additivity conjectures

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ and Ψ are quantum channels, is it true thar
$S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$.

This would be implied (taking $p \to 1$) by the following

$$\max_{\rho} \|(\Phi \otimes \Psi)(\rho)\|_p = \max_{\rho} \|\Phi(\rho)\|_p \max_{\rho} \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$.
3. (Hastings) Random counterexamples to the additivity conjecture ! Uses sharp results on the entropy of X^*X, where X uniformly distributed on the Hilbert–Schmidt sphere in $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$.

Additivity conjectures

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ and Ψ are quantum channels, is it true thar $S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$.

This would be implied (taking $p \to 1$) by the following

$$\max_\rho \|(\Phi \otimes \Psi)(\rho)\|_p = \max_\rho \|\Phi(\rho)\|_p \max_\rho \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$.
3. (Hastings) Random counterexamples to the additivity conjecture ! Uses sharp results on the entropy of X^*X, where X uniformly distributed on the Hilbert–Schmidt sphere in $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$.

Additivity conjectures

An important question is to decide wheter S_{min} is additive

Question (Additivity conjecture)

If Φ and Ψ are quantum channels, is it true thar $S_{\min}(\Phi \otimes \Psi) = S_{\min}(\Phi) + S_{\min}(\Psi)$.

This would be implied (taking $p \to 1$) by the following

$$\max_\rho \|(\Phi \otimes \Psi)(\rho)\|_p = \max_\rho \|\Phi(\rho)\|_p \max_\rho \|\Psi(\rho)\|_p. \tag{3}$$

1. (Winter) The existence of ε-randomizing channels with low Kraus rank implies that (3) is false for $p > 2$.
2. (Hayden–Winter) Applying Dvoretzky's theorem in $S_{2p}(\mathbf{C}^d, \mathbf{C}^N)$ gives counterexamples to (3) for any $p > 1$.
3. (Hastings) Random counterexamples to the additivity conjecture ! Uses sharp results on the entropy of X^*X, where X uniformly distributed on the Hilbert–Schmidt sphere in $\mathcal{M}(\mathbf{C}^d, \mathbf{C}^N)$.