Almost depolarizing channels with short Kraus decompositions

Guillaume AUBRUN

Université Lyon 1, France

Completely positive maps

$\mathcal{M}(\mathbf{C}^d)$: $d \times d$ complex matrices — $\langle A, B \rangle = \operatorname{Tr} AB^*$.

Definition (equivalent to the usual one)

A linear map $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ is **completely positive** *(CP) if there is a random matrix $V : (\Omega, \mathbf{P}) \to \mathcal{M}(\mathbf{C}^d)$ so that*

$$\Phi(X) = \mathbf{E} VXV^*.$$

- Depends only on the covariance matrix of V ($\in \mathcal{M}_+(\mathcal{M}(\mathbf{C}^d))$.
- Therefore V can be chosen to be finitely supported.

Kraus decomposition. Any CP $\Phi : \mathcal{M}(\mathbf{C}^d) \to \mathcal{M}(\mathbf{C}^d)$ can be decomposed as a sum of Kraus operators

$$\Phi(X) = \sum_{i=1}^{N} V_i X V_i^* \qquad \text{with } N \leqslant d^2.$$

The length N measures the complexity of Φ.

Quantum channels

Definition

A **state** $\rho \in \mathcal{M}(\mathbf{C}^d)$ *is a positive self-adjoint matrix with trace 1. The state* $\frac{\mathrm{Id}}{d}$ *(the* **maximally mixed state***) plays a central role.*

Definition

A CP map $\Phi : X \to \mathbf{E} VXV^*$ *is a* **quantum channel** *if it preseves trace*

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

- A quantum channel maps states to states.
- If V is supported in the unitary group $\mathcal{U}(d)$, then Φ is a quantum channel — not all quantum channels are like this.
- **A canonical example**. Let U be Haar-distributed on $\mathcal{U}(d)$. This leads to the « depolarizing » or « randomizing » channel Ψ.

$$\Psi(X) = \mathbf{E} UXU^* = \operatorname{Tr} X \frac{\mathrm{Id}}{d}.$$

Kraus decompositions of the depolarizing channel

Since the covariance matrix of U ($=$ a multiple of identity) has full rank, any Kraus decomposition of Ψ has length at least d^2.

Example : if $\omega = \exp(2i\pi/d)$, let A, B defined as

$$A(e_j) = \begin{bmatrix} \omega & & & 0 \\ & \omega^2 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}, \quad B(e_j) = \begin{bmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 1 & & & 0 \end{bmatrix}.$$

The set $\mathcal{U} = \{A^k B^l\}_{1 \leqslant k,l \leqslant d}$ is a orthogonal family of unitary matrices.

$$\Psi(X) = \operatorname{Tr} X \frac{\mathrm{Id}}{d} = \frac{1}{d^2} \sum_{k,l=1}^{d} A^k B^l X (A^k B^l)^*.$$

ε-randomizing channels

- Kraus decompositions of $\Psi \longleftrightarrow$ Exact encryption protocols.
- Approximate decomposition of $\Psi \longleftrightarrow$ Approximate encryption protocols.

Definition (Hayden, Leung, Shor and Winter)

A quantum channel $\Phi : \mathbf{C}^d \to \mathbf{C}^d$ is ε-randomizing if for any state ρ

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

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

- The depolarizing channel Ψ is 0-randomizing, but has Kraus decompositions of length d^2.
- Problem: find ε-randomizing channels with short Kraus decompositions (low-cost encryption).

Short random Kraus decompositions

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 $N \geqslant Cd \log d/\varepsilon^2$.
- **Idea of the proof :** For unit vectors $x, y \in \mathbf{C}^d$, the random variable $\langle x, Uy \rangle$ is subgaussian. Therefore a net argument coupled with Bernstein inequalities will work.
- Optimal dependence in d. Can we achieve better dependence in ε with another (non-random) construction ?

Derandomization

The Haar measure is hard to generate in real-life situations. We show (answering a question of HLSW) that we can replace « reduce the amount of randomness » and replace it by any measure.

Theorem

Let $U : (\Omega, \mathbf{P}) \to \mathcal{U}(d)$ be a random unitary matrix so that

$$\mathbf{E} UXU^* = \Psi(X) = \operatorname{Tr} X \cdot \frac{\mathrm{Id}}{d}.$$

Let (U_i) be i.i.d. copies of U. For $N \geqslant Cd(\log d)^6/\varepsilon^2$, the quantum channel

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

is ε-randomizing with probability $\geqslant 1/2$.

Isotropic measures

Definition

Say that a $\mathcal{U}(d)$-valued random vector U is **isotropic** *if*

$$\forall X \in \mathcal{M}(\mathbf{C}^d), \quad \mathbf{E}\, UXU^* = \operatorname{Tr} X \cdot \frac{\mathrm{Id}}{d},$$

$$\iff \forall X \in \mathcal{M}(\mathbf{C}^d), \quad \mathbf{E} |\operatorname{Tr} UX|^2 = \frac{1}{d} \|X\|_{\mathrm{HS}}^2.$$

1. Haar measure.
2. Uniform measure on $\mathscr{U}$ (orthogonal basis of unitary matrices).
3. On $\mathbf{C}^2$: uniform measure on the 4 Pauli matrices

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

4. On $(\mathbf{C}^2)^{\otimes k}$: k-wise tensor product of the previous example.

Examples 2-4 are not subgaussian $\longrightarrow$ net arguments cannot work.

Proof (1)

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

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

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

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

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 $B(S_\infty^d)$.

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.

Conclusion

Theorem

Let $(U_i) \in \mathcal{U}(d)$ be i.i.d. random matrices with isotropic law, and $N \geqslant Cd \log^6 d/\varepsilon^2$. With probability $\geqslant 1/2$,

$$\sup_{\rho \geqslant 0, \operatorname{Tr} \rho = 1} \left\| \frac{1}{N} \sum_{i=1}^{N} U_i \rho U_i^* - \frac{\mathrm{Id}}{d} \right\|_\infty \leqslant \frac{\varepsilon}{d}.$$

- The power of $\log d$ can certainly be improved, e.g. using Talagrand's majorizing measures instead of Dudley integral (however existing results in the litterature do not give better).
- You get $d \log^4 d$ if you prove the duality conjecture.
- However, some power of $\log d$ is needed, for example when U is distributed on a orthogonal set of unitary matrices.
- (Vague) question: is it possible to approximate any quantum channel (and not only Ψ) in a similar way ?