Seminar UV-UPV.
A quantitative no-programming theorem. Summary of terms and standard results.

Aleksander M. Kubicki

I. QUANTUM MODELS

We consider $\mathcal{H}, \mathcal{H}', \mathcal{K}$ finite dimensional complex Hilbert spaces, denoting $\mathcal{H} \simeq \mathbb{C}^d$, $\mathcal{H}' \simeq \mathbb{C}^{d'}$, $\mathcal{K} \simeq \mathbb{C}^k$. We will usually consider $\{e_i\}_{i=1}^d$ as an orthonormal basis on $\mathcal{H}$. Then, $\mathcal{L}(\mathcal{H})$ is the vector space of linear operators on $\mathcal{H}$.

Definition 1. *We refer to a state as a linear operator $\rho \in \mathcal{L}(\mathcal{H})$ satisfying the conditions*

1. *ρ is positive,*

2. *ρ has trace one.*

Definition 2. *A quantum channel (or evolution) is a linear map*

$$\mathcal{E} : \mathcal{L}(\mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{H}'),$$

which is completely positive and trace preserving. We denote by $\mathrm{CPTP}(\mathcal{H}, \mathcal{H}')$ *the set of these maps.*

An important class of quantum channels are unitary *channels, which acts by unitary conjugation*

$$\begin{array}{rccc} \mathcal{E} : & \mathcal{L}(\mathcal{H}) & \longrightarrow & \mathcal{L}(\mathcal{H}) \\ & \rho & \mapsto & U\,\rho\,U^\dagger, \end{array}$$

where $U \in \mathcal{L}(\mathcal{H})$ is a unitary operator.

Theorem 1 (Stinespring dilation)**.** *Let $\mathcal{E} : \mathcal{L}(\mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{H}')$ be a completely positive and trace preserving linear map. Then, there exist $k \in \mathbb{N}$, a unitary $U \in \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^k)$ and a state $\phi \in \mathcal{L}(\mathcal{H})$ such that*

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathbb{C}^k} U\,(\rho \otimes \phi)\,U^\dagger.$$

Definition 3. *A Positive Operator Valued Measurement, POVM, is a family of operators $\{E_j\}_{j=1}^m$, $E_j \in \mathcal{L}(\mathcal{H})$, which*

1. *are positive*

2. *and decompose the identity, $\mathrm{Id}_{\mathcal{H}} = \sum_{j=1}^m E_j$.*

Given a state ρ, the probability that the outcome of the POVM is j is given by $\mathrm{Tr}(E_j\,\rho)$.

II. STATE DISTINGUISHABILITY

Task: a state is received under the hypothesis that it is ρ_1 or ρ_2, with probability $1/2$ each. How well can we distinguish between both possibilities?

Definition 4. *Given a dichotomic POVM $\mathcal{M} = \{E_1, E_2\}$, we define the probability of distinguishing the states ρ_1 and ρ_2 using $\mathcal{M}$ as:*

$$p_{dist}^{\mathcal{M}}(\rho_1, \rho_2) := \frac{1}{2}\operatorname{Tr}(E_1 \cdot \rho_1) + \frac{1}{2}\operatorname{Tr}(E_2 \cdot \rho_2).$$

Therefore, the optimal probability of distinguishing the states ρ_1 and ρ_2 is the optimization of the former one over any possible POVM:

$$p_{dist}^{*}(\rho_1, \rho_2) = \sup_{\substack{\mathcal{M}=\{E_1, \mathrm{Id}-E_1\} \\ 0 \leq E_1 \leq \mathrm{Id}}} p_{dist}^{\mathcal{M}}(\rho_1, \rho_2).$$

Theorem 2 (Helström)**.**

$$\boxed{p_{dist}^{*} = \frac{1}{2} + \frac{1}{4}\|\rho_1 - \rho_2\|_1.}$$

Above, for $T \in \mathcal{L}(\mathcal{H})$, $\|T\|_1$ is the *trace norm* of T, defined as the ℓ_1 norm of the singular values of T. We denote the space of operators on $\mathcal{H}$ endowed with the trace norm as $\mathcal{S}_1(\mathcal{H})$.

III. CHANNEL DISTINGUISHABILITY

We promote the former discussion to the level of *evolutions*.

Task: a box is received under the hypothesis that on a state under our choice, it applies a quantum channel $\mathcal{E}_1$ or $\mathcal{E}_2$, with probability $1/2$ each. How well can we distinguish between both possibilities?

Definition 5. *Given a state $\rho \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$, and a dichotomic POVM $\mathcal{M} = \{E_1, E_2\}$, where $E_i \in \mathcal{L}(\mathcal{H} \otimes \mathcal{K})$, we define the probability of distinguishing the channels $\mathcal{E}_1$ and $\mathcal{E}_2$ using ρ and $\mathcal{M}$ as:*

$$q_{dist}^{\rho,\mathcal{M}}(\rho_1, \rho_2) := \frac{1}{2}\operatorname{Tr}\left((\mathcal{E}_1 \otimes \mathrm{Id}_{\mathcal{K}}) \cdot \rho\right) + \frac{1}{2}\operatorname{Tr}\left((\mathcal{E}_2 \otimes \mathrm{Id}_{\mathcal{K}}) \cdot \rho_2\right).$$

Therefore, the optimal probability of distinguishing the channels $\mathcal{E}_1$ and $\mathcal{E}_2$ is:

$$p_{dist}^{*}(\rho_1, \rho_2) = \sup_{\mathcal{K}} \sup_{\substack{\mathcal{M}=\{E_1, \mathrm{Id}-E_1\} \,:\, 0 \leq E_1 \leq \mathrm{Id} \\ \rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{K})}} q_{dist}^{\rho,\mathcal{M}}(\mathcal{E}_1, \mathcal{E}_2),$$

where $\mathcal{K}$ in the first supremum is a finite dimensional Hilbert space.

Theorem 3.

$$\boxed{q_{dist}^{*} = \frac{1}{2} + \frac{1}{4}\|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond}.}$$

Above, for any $\mathcal{T} : \mathcal{L}(\mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{H})$, $\|\mathcal{T}\|_{\diamond}$ is the *diamond norm* defined as:

$$\|\mathcal{T}\|_{\diamond} := \sup_{\mathcal{K}} \left\|\mathcal{T} : \mathcal{S}_1(\mathcal{H} \otimes \mathcal{K}) \longrightarrow \mathcal{S}_1(\mathcal{H} \otimes \mathcal{K})\right\|,$$

where $\mathcal{K}$ is restricted to be a finite dimensional Hilbert space.

IV. UNIVERSAL PROGRAMMABLE QUANTUM PROCESSORS

Definition 6. *A quantum channel $\mathcal{P} \in \mathrm{CPTP}(\mathcal{H} \otimes \mathcal{H}_M)$ is a d-dimensional Universal Programmable Quantum Processor,* UPQP_d*, if* $\dim \mathcal{H} = d$ *and for every $U \in \mathcal{U}(\mathcal{H})$ there exists a unit vector $|\phi_U\rangle \in \mathcal{H}_M$ such that:*

$$\mathrm{Tr}_{\mathcal{H}_M}\left[\mathcal{P}\left(\rho \otimes |\phi_U\rangle\langle\phi_U|\right)\right] = U\rho U^\dagger, \quad \textit{for every} \;\; \rho \in \mathcal{D}(\mathcal{H}).$$

Definition 7. *We say that $\mathcal{P} \in \mathrm{CPTP}(\mathcal{H} \otimes \mathcal{H}_M)$ is a d-dimensional ε–Universal Programmable Quantum processor, $\varepsilon -$* UPQP_d*, if* $\dim \mathcal{H} = d$ *and for every $U \in \mathcal{U}(\mathcal{H})$ there exists a unit vector $|\phi_U\rangle \in \mathcal{H}_M$ such that:*

$$\frac{1}{2}\left\| \mathrm{Tr}_{\mathcal{H}_M}\left[\mathcal{P}\left(\;\cdot\; \otimes |\phi_U\rangle\langle\phi_U|\right)\right] \;-\; U \cdot U^\dagger \right\|_\diamond \leq \varepsilon,$$

where $\|\;\cdot\;\|_\diamond$ denotes the diamond norm.

V. OPERATOR SPACES AND THE CB NORM

From now on, we denote as M_k the linear space of $k \times k$ complex matrices endowed with the operator norm (i.e., viewed as operators on the Hilbert space $\mathbb{C}^k$). In general, for any Hilbert space $\mathcal{H}$, we denote as $\mathcal{B}(\mathcal{H})$ the Banach space of linear operators on $\mathcal{H}$ with the norm given by the operator norm.

An operator space is a complex Banach space E together with a sequence of "reasonable" norms in the spaces $M_k \otimes E = M_k(E)$, where $M_k(E)$ is the space of square matrices of order k with entries in E. This turns out to be equivalent to the following:

Definition 8. *An operator space, E, is a closed subspace of some $\mathcal{B}(\mathcal{H})$, $E \subset \mathcal{B}(\mathcal{H})$. The norm in $M_k(E)$ is determined as the norm inherited from the embedding $M_k(E) \subset M_k(\mathcal{B}(\mathcal{H})) \simeq \mathcal{B}(\mathbb{C}^k \otimes \mathcal{H})$.*

The natural morphisms between these objects are no longer bounded linear maps, but *completely bounded* linear maps:

Definition 9. *Given a linear map between operator spaces $\Phi : E \to F$, we define its completely bounded norm as $\|\Phi\|_{cb} := \sup_k \|\mathrm{Id}_{M_k} \otimes \Phi : M_k(E) \to M_k(F)\|$. We say that Φ is completely bounded if $\|\Phi\|_{cb} < \infty$. We denote the Banach space of completely bounded maps from E into F as $\mathcal{CB}(E, F)$.*

If $\Phi \otimes \mathrm{Id}_{M_k}$ is an isometry $\forall k \in \mathbb{N}$, we say that Φ is a complete isometry.

Completely bounded maps provides the notion of duality of an operator space E, E^*. For any $k \in \mathbb{N}$ we just define $M_k(E^*)$ as the space of linear operators $\mathcal{L}(E, M_k)$ endowed with the c.b. norm.

Example 1.

(i) There is a natural operator space structure on $\mathcal{B}(\mathcal{H})$ given by the identification $M_k(\mathcal{B}(\mathcal{H})) = \mathcal{B}(\mathbb{C}^k \otimes \mathcal{H})$.

(ii) Then, $\mathcal{S}_1(\mathcal{H})$ inherits its operator space structure from the former by duality.

Theorem 4. *The natural embedding*

$$\theta : \mathcal{B}(\mathcal{H} \otimes \mathcal{K}) \longrightarrow \mathcal{CB}(\mathcal{S}_1(\mathcal{H}), \mathcal{B}(\mathcal{K})),$$

determined by $\theta(U \otimes V)\,(T) = U(T)\,V \equiv \mathrm{Tr}(U\,T^t)\,V$, *where* $\cdot^t$ *is the transpose map, is a complete isometry.*

VI. TYPE/COTYPE OF A BANACH SPACE

To built the notion of type/cotype of a Banach space we need to introduce Rademacher random variables. These are random variables which takes de values -1 and 1 with equal probability $1/2$. Let us denote by $\{\varepsilon_i\}_{i=1}^n$ a set of n i.i.d. such random variables. Then, $\mathbb{E}[f(\{\varepsilon_i\}_{i=1}^n)]$ will be the expected value of the function f over any combination of signs $\{\varepsilon_i\}_{i=1}^n \in \{-1,1\}^n$ with uniform weight $1/2^n$.

Definition 10. *Let* X *be a Banach space and let* $1 \leq p \leq 2$. *We say* X *is of (Rademacher) type* p *if there exists a positive constant* T *such that for every natural number* n *and every sequence* $\{x_i\}_{i=1}^n \subset X$ *we have*

$$\left(\mathbb{E}\Big[\big\|\sum_{i=1}^n \varepsilon_i x_i\big\|_X^2\Big]\right)^{1/2} \leq \mathrm{T}\left(\sum_{i=1}^n \|x_i\|_X^p\right)^{1/p},$$

Moreover, we define the Rademacher type p *constant* $\mathrm{T}_p(X)$ *as the infimum of the constants* T *fulfilling the previous inequality.*

For the sake of completeness we will also introduce, for a given Banach space X and $2 \leq q < \infty$, the Rademacher cotype q constant $\mathrm{C}_q(X)$ as the infimum of the constant C (in case they exist) such that the following inequality holds for every natural number n and every sequence $\{x_i\}_{i=1}^n \subset X$,

$$\mathrm{C}^{-1}\Big(\sum_{i=1}^n \|x_i\|_X^q\Big)^{1/q} \leq \left(\mathbb{E}\Big[\big\|\sum_{i=1}^n \varepsilon_i x_i\big\|_X^2\Big]\right)^{1/2}$$

Proposition 1. *Given a linear isomorphism between two Banach spaces* X *and* Y, $\Phi : X \to Y$, *the following relation between type constants holds:*

$$\mathrm{T}_p(X) \leq \|\Phi\|\|\Phi^{-1}\|\mathrm{T}_p(Y).$$

Proposition 2. $\mathrm{T}_p(X)$ *is preserved by subspaces. That is, if* S *is a subspace of* X *(as Banach spaces), then* $\mathrm{T}_p(S) \leq \mathrm{T}_p(X)$.

Fact 1.

$$\mathrm{T}_2(\mathcal{S}_1(\mathbb{C}^d)) \geq d^{1/2}, \qquad \mathrm{T}_2(\mathcal{B}(\mathbb{C}^d)) \leq (C\log(d))^{1/2}.$$

	Previous results		This work	
Lower bounds	$m \geq \mathsf{K}(\frac{1}{d})^{\frac{d+1}{2}} \left(\frac{1}{\varepsilon}\right)^{\frac{d-1}{2}}$	[1]	$m \geq 2^{\frac{(1-\varepsilon)}{\mathsf{K}} d - \frac{2}{3}\log d}$	[3, Th. 3]
	$m \geq \mathsf{K}\left(\frac{d}{\varepsilon}\right)^2$	[2]		
Upper bounds	$m \leq 2^{\frac{4d^2 \log d}{\varepsilon^2}}$	[2, 4, 5]	$m \leq \left(\frac{\mathsf{K}}{\varepsilon}\right)^{d^2}$	[3, Eq.2]

TABLE I. Best known bounds for the optimal memory size of UPQPs in comparison with the results presented here. Above, K denotes universal constants, not necessarily equal between them. Let us point out that the bound from [1] was deduced for programmable measurements instead of UPQPs. However, since a UPQP always can be turned into a Universal Programmable Quantum Measurement, this lower bound also applies for the case studied here. Notice that the alluded bound, although it enforces a strong scaling of m with ε, becomes trivial for large input dimension d. It is in this regime where the bound from [2] is more informative, but still exponentially weaker than the bound provided by Theorem [3, Th. 3].

VII. SOME COMMENTS ON BIBLIOGRAPHY

A. Quantum Information Theory

The standard reference in this field is [6] (so far, it was cited almost 35 000 times on Google Scholar!), but it was written twenty years ago and i would say that the presentation is getting a bit outdated and it is written for physicist. Then, for more modern and mathematically oriented introductions to Quantum Information Theory, i suggest the books [7], [8] (both are available online for free). For an introduction to Quantum Information Theory from Classical Shannon's theory, see [9].

B. Operator Spaces

Standard references on Operator Space Theory are [10, 11]. See [12, 13] for some recent connections between Operator Space Theory and Quantum Information.

[1] D. Pérez-García, Phys. Rev. A **73**, 052315 (2006).
[2] C. Majenz, *Entropy in quantum information theory - Communication and cryptography*, Ph.D. thesis (2017).
[3] A. M. Kubicki, C. Palazuelos, and D. Pérez-García, arXiv:1805.00756 (2018).
[4] S. Ishizaka and T. Hiroshima, Phys. Rev. Lett. **101**, 240501 (2008).
[5] S. Beigi and R. König, New Journal of Physics **13**, 093036 (2011).
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).
[7] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).
[8] G. Aubrun and S. J. Szarek, *Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory* (American Mathematical Society, 2017).
[9] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
[10] E. G. Effros and Z.-J. Ruan, *Operator Spaces* (Oxford University Press, 2000).

[11] G. Pisier, *Introduction to Operator Space Theory*, London Mathematical Society Lecture Note Series (Cambridge University Press, 2003).

[12] V. Prakash Gupta, P. Mandayam, and V. Sunder, *The Functional Analysis of Quantum Information Theory, A Collection of Notes Based on Lectures by Gilles Pisier, K. R. Parthasarathy, Vern Paulsen and Andreas Winter* (Springer, 2015).

[13] C. Palazuelos and T. Vidick, Journal of Mathematical Physics **57**, 015220 (2016), https://doi.org/10.1063/1.4938052.