ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 7

HS 11
Prof. M. Christandl

Exercise 7.1 Fast matrix multiplication

Can quantum information help us find ways of multiplying matrices in classical computers using less resources (bit operations)?

a) We can always represent matrices as vectors,

$$M = \sum_{ij} \lambda_{ij}\ |a_i\rangle\langle b_j| \in \mathrm{Hom}(\mathcal{H}_B, \mathcal{H}_A) \quad \leftrightarrow \quad |M\rangle = \sum_{ij} \lambda_{ij}\ |a_i\rangle|b_j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B, \quad \text{e.g.,} \begin{pmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \quad \leftrightarrow \quad \begin{pmatrix} \lambda_{11} \\ \lambda_{12} \\ \lambda_{21} \\ \lambda_{22} \end{pmatrix}.$$

Let A and B be two 2×2 matrices,

$$A = \sum_{i,j=0}^{1} a_{ij}\ |a_i\rangle\langle a_j| \in \mathrm{Hom}(\mathcal{H}_{A'}, \mathcal{H}_A), \qquad\qquad B = \sum_{k,\ell=0}^{1} b_{k\ell}\ |b_k\rangle\langle b_\ell| \in \mathrm{Hom}(\mathcal{H}_{B'}, \mathcal{H}_B),$$

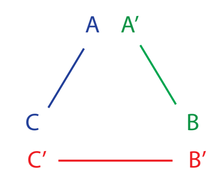
Represent A, B and AB as vectors. How many multiplications of input variables do you have to do to obtain AB?

Note 1: To keep track of all the different spaces, use $|A\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$, $|B\rangle \in \mathcal{H}_B \otimes \mathcal{H}_{B'}$ and $|AB\rangle \in \mathcal{H}_C \otimes \mathcal{H}_{C'}$. Use a basis $\{|c_0\rangle, |c_1\rangle\}$ for $\mathcal{H}_C$.
Note 2: the vector representations of operators are not necessarily normalized.

b) Represent matrix multiplication as an operator

$$E \in \mathrm{Hom}\Big((\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'}),\ \mathcal{H}_C \otimes \mathcal{H}_{C'}\Big) : E\ [\ |A\rangle \otimes |B\rangle\ ] = |AB\rangle.$$

c) The next step is to represent E as a vector $|E\rangle \in (\mathcal{H}_C \otimes \mathcal{H}_{C'}) \otimes (\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'})$. Verify that $|E\rangle$ is the (non-normalized) tensor product of three maximally entangled states:



d) *Tensor rank* is a generalization of the Schmidt rank for multipartite systems. The tensor rank of a vector $|\psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ is defined as the smallest r such that we can write

$$|\psi\rangle = \sum_{m=1}^{r} |\phi_1^m\rangle_{\mathcal{H}_1} \otimes |\phi_2^m\rangle_{\mathcal{H}_2} \otimes \cdots \otimes |\phi_N^m\rangle_{\mathcal{H}_N}.$$

Note that the vectors $\{|\phi_i^m\rangle\}_m$ do not need to be orthogonal. We are interested in the tensor rank of $|E\rangle$, i.e., the smallest r such that

$$|E\rangle = \sum_{m=1}^{r} |\tau_m\rangle_{CC'}\ |\psi_m\rangle_{AA'}\ |\phi_m\rangle_{BB'}.$$

Show that $4 \le r \le 8$.

e) Strassen showed that in fact $r \le 7$ (you can try to prove this for an extra 20 points). This means that we can write E as

$$E = \sum_{m=1}^{7} |\tau_m\rangle_{CC'} \langle\psi_m|_{AA'} \langle\phi_m|_{BB'}.$$

Compute $E(|A\rangle|B\rangle)$, for this representation of E. How many multiplications of input variables did you have to perform now? Note that the vectors $\{|\tau_m\rangle, |\psi_m\rangle, |\phi_m\rangle\}_m$ are always the same, independently of the actual matrices A and B.

Exercise 7.2 Unambiguous state discrimination

Suppose you are given one of two states, ρ and σ, with equal probability, and want to distinguish them with a single measurement. We have seen that, unless the states are orthogonal ($\delta(\rho,\sigma)=1$), it is impossible to always distinguish them with certainty. We also saw that if you wanted to maximize the probability of guessing correctly, the best strategy was to measure the state in the eigenbasis of $\rho-\sigma$: you would be right with probability $\Pr_{\checkmark}=\frac{1}{2}(1+\delta(\rho,\sigma))$.

Now suppose you have a different goal: you will only make a guess when you are certain of which state you have, so as to never make a mistake. Formally, you will perform a measurement described by a POVM $\{M_\rho, M_\sigma, M_?\}$, such that: (1) if you obtain an outcome corresponding to M_ρ or M_σ, you know for sure that you have ρ or σ, respectively, and (2) if your outcome corresponds to $M_?$ you do not know with certainty which state you have, and you will not risk guessing.

a) We will consider only pure states $\rho=|\psi\rangle\langle\psi|, \sigma=|\phi\rangle\langle\phi|$. We want to have zero probability of guessing "ψ" when the state measured was ϕ (and vice-versa) . What does this tell us about the form of M_ψ, M_ϕ and $M_?$?

b) Now we want to maximize the probability of making a correct guess, i.e., to minimize the probability of obtaining $M_?$. Do so. ☺ Remember that you can expand one of the states in terms of the other and a vector orthogonal to it, for instance

$$|\psi\rangle = a|\phi\rangle + b|\phi^\perp\rangle, \quad |\psi^\perp\rangle = -b|\phi\rangle + a|\phi^\perp\rangle, \qquad a=\langle\psi|\phi\rangle, \quad |a|^2+|b|^2=1.$$

c) What happens if ψ and ϕ are given with probability q and $1-q$?

Exercise 7.3 Distinguishing channels

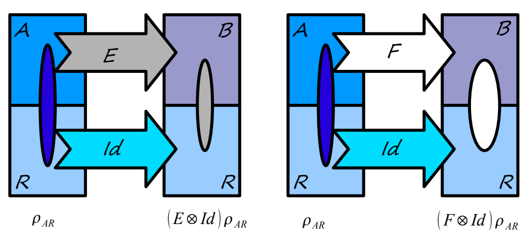
We have seen that TPCPMs may be used to define channels. Now let's see how to quantify similarity between two channels. Consider two TPCPMs $\mathcal{E},\mathcal{F}:\mathrm{End}(\mathcal{H}_A)\mapsto\mathrm{End}(\mathcal{H}_B)$.
A naive approach is to send the same state through each of the channels and see how similar the output states are,

$$d(\mathcal{E},\mathcal{F}) = \max_{\rho_A}\delta(\mathcal{E}(\rho_A),\mathcal{F}(\rho_A)), \tag{1}$$

where $\delta(\rho,\sigma)$ is the trace distance between states.
However, we may want to consider that ρ_A may be entangled with some other system, and therefore a channel that acts locally may produce global changes on the total state (for instance break the entanglement). The stabilized distance takes that into account:

$$d^\diamond(\mathcal{E},\mathcal{F}) = \max_{\rho_{AR}}\delta(\mathcal{E}\otimes\mathcal{I}(\rho_{AR}),\mathcal{F}\otimes\mathcal{I}(\rho_{AR})), \tag{2}$$

where $\mathcal{I}$ is the identity map.



a) Show that in general $d(\mathcal{E},\mathcal{F})\le d^\diamond(\mathcal{E},\mathcal{F})$.

b) Consider the fully depolarising channel on one qubit, $\mathcal{E}_p(\rho)=p\frac{\mathbb{1}}{2}+(1-p)\rho$, that can be expressed in the operator-sum representation ($\mathcal{E}(\rho)=\sum_k E_k\rho {E_k}^\dagger$) with the operators $\sqrt{1-\frac{3p}{4}}\,\mathbb{1}$ and $\frac{\sqrt{p}}{2}\sigma_i, \quad i=x,y,z$.
Compute and compare $d(\mathcal{E}_p,\mathcal{I})$ and $d^\diamond(\mathcal{E}_p,\mathcal{I})$.

c) Find an example of two channels $\mathcal{E},\mathcal{F}$ for which the two distance measures are very different.

Exercise 7.4 Seriously. (1 point)

Come up with a good Schrödinger/Heisenberg joke. You can try to improve the following, or make a new one. Schrödinger and Heisenberg meet at a cocktail party. Schrödinger says "you're old!" Heisenberg replies "no, my friend, you are."