Exercise Sheet 10: Bernstein-Vazirani and Grover

The Bernstein-Vazirani algorithm

Here, we will work through a simple quantum algorithm that achieves something that is classically impossible: It learns an unknown n-bit string using only a single "quantum query" to the string.

7 P. **Exercise 1.** The Bernstein-Vazirani problem is as follows: You are given access to a unitary U_s that acts on the computational basis as $U_s|x, b\rangle = |x, b \oplus s \cdot x\rangle$, $x \in \{0,1\}^n$, $b \in \{0,1\}$, where $\oplus$ denotes addition modulo 2, $\cdot$ denotes the inner product of two n-bit strings (again with addition modulo 2), and where $s \in \{0,1\}^n$ is an unknown n-bit string. Identify s using as few queries to U_s as possible.

2 P. (a) Show that U_s can simulate the unitary $\tilde{U}_s$ that acts as on the computational basis as $\tilde{U}_s|x\rangle = (-1)^{s \cdot x}|x\rangle$. That is, show that a single use of U_s suffices to implement a single use of $\tilde{U}_s$.

Hint: What happens if you apply U_s to $|x\rangle \otimes |-\rangle$?

Solution

By direct computation, we see that

$$\begin{aligned} U_s(|x\rangle \otimes |-\rangle) &= \frac{1}{\sqrt{2}} \left(U_s|x,0\rangle - U_s|x,1\rangle\right) \\ &= \frac{1}{\sqrt{2}} \left(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle\right) \\ &= |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) = \begin{cases} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ |x\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases} \\ &= |x\rangle \otimes (-1)^{f(x)}|-\rangle \\ &= (-1)^{f(x)}|x\rangle \otimes |-\rangle\,. \end{aligned}$$

Thus, we can simulate a single use of $\tilde{U}_s$ on input $|x\rangle$ with a single use of U_s as follows: "Attach" a tensor factor $|-\rangle$ (which, if you want to start from $|0\rangle$, you can get by applying HX), apply U_s to the composite system, then trace out the "attached" subsystem.

3 P. (b) Recall the Hadamard gate H from Exercise Sheet 8. Show that $H^{\otimes n}\tilde{U}_s H^{\otimes n}|0^n\rangle = |s\rangle$.

Hint: Remember that $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{t \in \{0,1\}^n} (-1)^{t \cdot x}|t\rangle$, where the sums in the inner products $t \cdot x$ are modulo 2. Also, in your proof, you may want to use the identity $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{y \cdot x} = \delta_{y,0^n}$.

Solution

By definition of the Hadamard gate, the action of $H^{\otimes n}$ on the computational basis is $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{t\in\{0,1\}^n} (-1)^{t\cdot x}|t\rangle$. In particular, $H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$. Thus, we get $\tilde{U}_s H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x}|x\rangle$. It remains to include the last layer of Hadamard gates:

$$\begin{aligned} H^{\otimes n}\tilde{U}_s H^{\otimes n}|0^n\rangle &= H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x}|x\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x} H^{\otimes n}|x\rangle \\ &= \sum_{t\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{(s\oplus t)\cdot x} \right) |t\rangle \,. \end{aligned}$$

Now, observe that

$$\begin{aligned} \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{y\cdot x} &= \prod_{i=1}^n \left(\frac{1}{2} \sum_{x_i\in\{0,1\}} (-1)^{y_i x_i} \right) \\ &= \prod_{i=1}^n (\delta_{y_i,0}) \\ &= \delta_{y,0^n} \,. \end{aligned}$$

Plugging this into our computation above, we get

$$\begin{aligned} H^{\otimes n}\tilde{U}_s H^{\otimes n}|0^n\rangle &= \sum_{t\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{(s\oplus t)\cdot x} \right) |t\rangle \\ &= \sum_{t\in\{0,1\}^n} \underbrace{\delta_{s\oplus t,0^n}}_{\delta_{s,t}} |t\rangle \\ &= |s\rangle \,. \end{aligned}$$

2 P. (c) Using (a) and (b), describe a protocol that solves the Bernstein-Vazirani problem with a single query to U_s. How many single-qubit quantum gates are sufficient to implement your protocol assuming all qubits start in $|0\rangle$ (ignoring U_s, because we imagine somebody else is implementing that for you)?

Solution

Start with $|0^n\rangle$. First apply $H^{\otimes n}$. Then, via (a), implement $\tilde{U}_s$ using one query to U_s. Afterwards, apply $H^{\otimes n}$ and measure all qubits in the computational basis. Because of (b), the observed string of outcomes will exactly be s.

Let's count gates. We immediately see that we have $2n$ single-qubit Hadamard gates. Additionally, to get from U_s to $\tilde{U}_s$, we need one single-qubit gate (HX, as discussed in (a)) that maps $|0\rangle$ to $|-\rangle$. So, $2n+1$ single-qubit gates are sufficient overall.

In the following bonus exercise, you can convince yourself of the fact that any classical procedure for solving (the classical analog of) the Bernstein-Vazirani problem needs to make linearly-in-n many queries to the unknown bit string.

3 P. **Bonus Exercise 1.** Consider the following classical version of the Bernstein-Vazirani problem: You are given query access to the function $\{0,1\}^n \ni x \mapsto s \cdot x$ for some unknown n-bit string $s \in \{0,1\}^n$. Here, a single query consists of you choosing an input $x \in \{0,1\}^n$ and receiving the output $s \cdot x \in \{0,1\}$. Identify s with as few queries to the function as possible.

In this exercise, we show that any classical algorithm that solves this problem with success probability $\geq 2/3$ has to make at least n many queries. This is to be contrasted with the quantum solution from Exercise 1, which achieves success probability 1 with a single quantum query.

2 P. (a) Suppose the first q queries of the algorithm lead to data $(x_1, s\cdot x_1), \ldots, (x_q, s\cdot x_q)$. Further assume that the largest linearly independent subset of $\{x_1, \ldots, x_q\}$ has size $\ell \leq q$. Argue that the set $\{t \in \{0,1\}^n \mid t \cdot x_i = s \cdot x_i \ \forall 1 \leq i \leq q\}$ of all candidate strings that are consistent with the data has size $2^{n-\ell}$.

Solution

The dataset imposes q many linear constraints on the unknown string. By assumption, only ℓ of those are linearly independent. So, the set $\{t \in \{0,1\}^n \mid t \cdot x_i = s \cdot x_i \ \forall 1 \leq i \leq q\}$ is an affine subspace of dimension $n - \ell$. Thus, as we are over the field $\{0,1\}$, that set has cardinality $2^{n-\ell}$.

1 P. (b) Conclude from (a) that any classical algorithm that solves our problem of interest with success probability $\geq 2/3$ has to make at least n many queries.

Solution

Suppose the classical algorithm makes m many, possibly randomized, queries. After those queries, the algorithm holds a dataset $(x_1, s\cdot x_1), \ldots, (x_m, s\cdot x_m)$. In particular, the largest linearly independent subset of $\{x_1, \ldots, x_m\}$ has size at most m. So, by (a), after those queries, there are still at least 2^{n-m} many candidate strings left. The best the algorithm can now do is to guess uniformly at random among those, then its success probability is 2^{m-n}. Requiring this to be $\geq 2/3$, we can rearrange and get $m \geq n - \log(3/2)$. As m has to be an integer and since $\log(3/2) < 1$, this implies $m \geq n$.

Clearly, n classical queries, even deterministic ones, also suffice to solve the classical analogue of Bernstein-Vazirani: Simply query $e_1, \ldots, e_n$ for the unit basis vectors to learn the n entries of the unknown string s.

Grover, one step further

10 P. **Exercise 2.** In this exercise we want to expand on what we learned in the lecture about Grover's algorithm, and extend the results to the case of multiple marked elements. Remember, Grover's algorithm allows to find the one marked element in a list of N elements in $O(\sqrt{N})$ queries. Now, we want to see what happens if there are M marked elements.

Let us call S the set of marked elements, so $S \subset \{0,1\}^n$, with $|S| = M$ and $1 < M \ll N$. With that, let us first name the two main states of the derivation

$$\text{uniform superposition} \qquad |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$$\text{marked superposition} \qquad |S\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle\,.$$

Then, let us redefine the database operator

$$U_S = \mathbb{I} - 2\Pi_S \quad \text{with} \quad \Pi_S = \sum_{x \in S} |x\rangle\langle x| \,.$$

Note that here, in contrast to the $M = 1$ case, $U_S \neq \mathbb{I} - 2|S\rangle\langle S|$. Just as in the $M = 1$ case however, the algorithm consists of initializing the state in $|\Psi\rangle$ and then repeatedly applying the Grover operator $G = U_\Psi U_S$, where $U_\Psi = 2|\Psi\rangle\langle\Psi| - \mathbb{I}$, until the state is close to the target state $|S\rangle$, and then measuring that.

2 P. (a) First, like in the case of only one marked element, we can restrict our attention to a two-dimensional subspace of states in which the algorithm acts. For that, show that, given the initial $|\Psi\rangle$ state, the repeated application of the Grover operator keeps the state in $\operatorname{span}\{|\Psi\rangle, |S\rangle\}$.

Hint: Look at the effect of U_S and U_Ψ on both $|\Psi\rangle$ and $|S\rangle$.

Solution

Let us start with U_Ψ.

$$U_\Psi|\Psi\rangle = (2|\Psi\rangle\langle\Psi| - \mathbb{I})|\Psi\rangle = 2|\Psi\rangle - |\Psi\rangle = |\Psi\rangle$$
$$U_\Psi|S\rangle = (2|\Psi\rangle\langle\Psi| - \mathbb{I})|S\rangle = 2\langle\Psi|S\rangle|\Psi\rangle - |S\rangle$$

In both cases, the output state is a linear combination of $|\Psi\rangle$ and $|S\rangle$, so it remains in the stated subspace. Now for U_S.

$$\begin{aligned} U_S|S\rangle = (\mathbb{I} - 2\Pi_S)|S\rangle &= |S\rangle - 2\left(\sum_{x\in S}|x\rangle\langle x|\right)\frac{1}{\sqrt{M}}\left(\sum_{x'\in S}|x'\rangle\right) \\ &= |S\rangle - \frac{2}{\sqrt{M}}\sum_{x\in S}|x\rangle = -|S\rangle \\ U_S|\Psi\rangle = (\mathbb{I} - 2\Pi_S)|\Psi\rangle &= |\Psi\rangle - 2\left(\sum_{x\in S}|x\rangle\langle x|\right)\frac{1}{\sqrt{N}}\left(\sum_{x'=0}^{N-1}|x'\rangle\right) \\ &= |\Psi\rangle - \frac{2}{\sqrt{N}}\sum_{x\in S}|x\rangle = |\Psi\rangle - \frac{2\sqrt{M}}{\sqrt{N}}|S\rangle \end{aligned}$$

Again, in both cases we have linear combinations of $|\Psi\rangle$ and $|S\rangle$. We can conclude that, if starting withing the span of $\{|\Psi\rangle, |S\rangle\}$, the application of the Grover operator will always return a state withing that subspace.
In case anyone is confused about the shape of the last state, one can verify it is a valid state by checking the normalization

$$\begin{aligned} \|U_S|\Psi\rangle\|_2^2 &= \left(\langle\Psi| - \frac{2}{\sqrt{N}}\sum_{x\in S}\langle x|\right)\left(|\Psi\rangle - \frac{2}{\sqrt{N}}\sum_{x'\in S}|x'\rangle\right) \\ &= \langle\Psi|\Psi\rangle - \frac{2}{\sqrt{N}}\sum_{x'\in S}\langle\Psi|x'\rangle - \frac{2}{\sqrt{N}}\sum_{x\in S}\langle x|\Psi\rangle + \left(\frac{2}{\sqrt{N}}\sum_{x\in S}\langle x|\right)\left(\frac{2}{\sqrt{N}}\sum_{x'\in S}|x'\rangle\right) \\ &= 1 - \frac{2}{\sqrt{N}}\sum_{x'\in S}\frac{1}{\sqrt{N}} - \frac{2}{\sqrt{N}}\sum_{x\in S}\frac{1}{\sqrt{N}} + \frac{4}{N}\sum_{x\in S}1 \\ &= 1 - \frac{2M}{N} - \frac{2M}{N} + \frac{4M}{N} = 1 \end{aligned}$$

2 P. (b) Show that in that subspace, U_Ψ acts as a reflection with respect to $|\Psi\rangle$ and U_S as an inversion with respect to $|S\rangle$ respectively. With reflection and inversion, we mean

$$\begin{array}{ll} \text{reflection} & R_\psi(\alpha|\psi\rangle + \beta|\psi^\perp\rangle) = \alpha|\psi\rangle - \beta|\psi^\perp\rangle \\ \text{inversion} & I_\psi(\alpha|\psi\rangle + \beta|\psi^\perp\rangle) = -\alpha|\psi\rangle + \beta|\psi^\perp\rangle\,. \end{array}$$

Hint: Decompose the state of interest into a basis of the space span$\{|\Psi\rangle, |S\rangle\}$*, choosing the basis carefuly.*

Solution

First U_Ψ. For any $|\phi\rangle \in \text{span}\{|\Psi\rangle, |S\rangle\}$ we can write it as a linear combination of $|\Psi\rangle$ and $|\Psi^\perp\rangle$ where $|\Psi^\perp\rangle$ is some state in span$\{|\Psi\rangle, |S\rangle\}$ such that $\langle\Psi|\Psi^\perp\rangle = 0$.

$$\begin{aligned} U_\Psi|\phi\rangle &= (2|\Psi\rangle\langle\Psi| - \mathbb{I})(\alpha|\Psi\rangle + \beta|\Psi^\perp\rangle) = 2\alpha|\Psi\rangle + 0 - \alpha|\Psi\rangle - \beta|\Psi^\perp\rangle \\ &= \alpha|\Psi\rangle - \beta|\Psi^\perp\rangle = R_\Psi|\phi\rangle\,. \end{aligned}$$

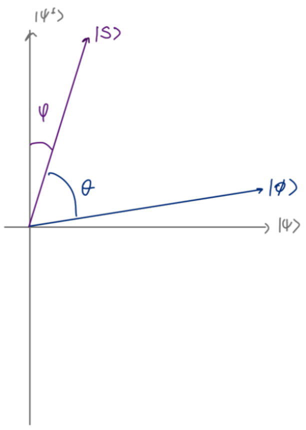
The $|\Psi\rangle$ component stayed unchanged, while the $|\Psi^\perp\rangle$ had a sign flip, thus it has been reflected with respect to $|\Psi\rangle$.

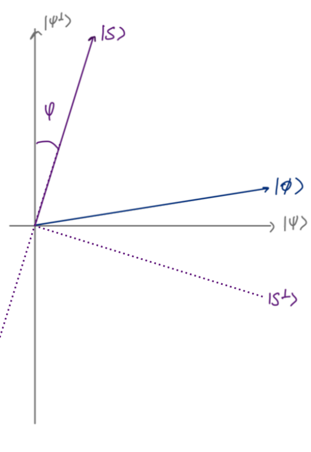
For U_S we can do the same, choosing the basis $\{|S\rangle, |S^\perp\rangle\}$. Here, $|S^\perp\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\notin S}|x\rangle$. Then, any state can be written $|\phi\rangle = \tilde{\alpha}|S\rangle + \tilde{\beta}|S^\perp\rangle$. We now want to show that $U_S|\phi\rangle = -\tilde{\alpha}|S\rangle + \tilde{\beta}|S^\perp\rangle$. The first term is easy, since we already showed in (a) that $U_S|S\rangle = -|S\rangle$. Then for the second

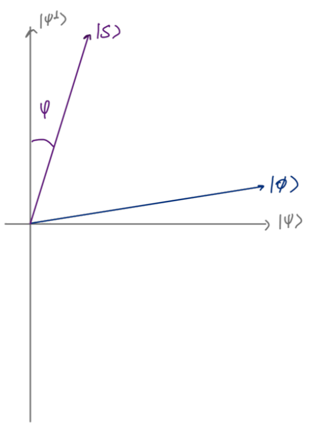
$$U_S|S^\perp\rangle = (\mathbb{I} - 2\Pi_S)\,|S^\perp\rangle = |S^\perp\rangle - 2\left(\sum_{x\in S}|x\rangle\langle x|\right)\frac{1}{\sqrt{N-M}}\sum_{x'\notin S}|x'\rangle = |S^\perp\rangle\,,$$

since all summands in the second part are zero, as $\langle x|x'\rangle = 0$ if $x \in S$ and $x' \notin S$.

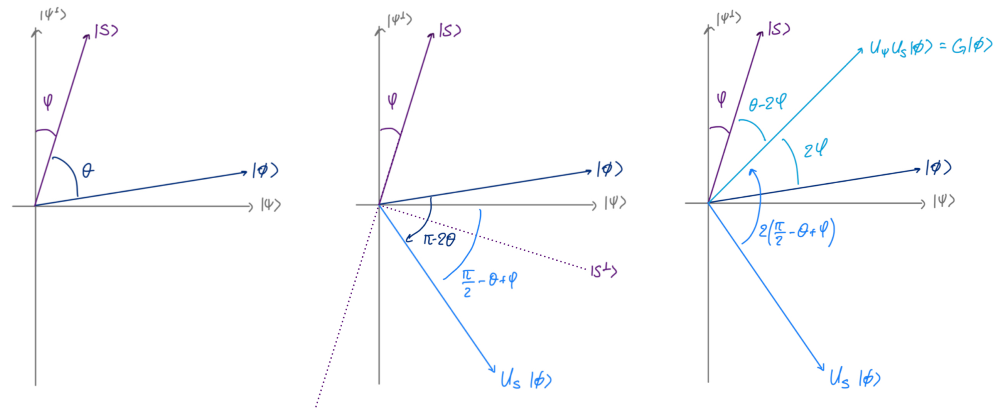
2 P. (c) Show on the following sketches the effect of U_S on the state $|\phi\rangle$ (second sketch) and then the effect of U_Ψ on the resulting state (third sketch). Give the angle between $U_\Psi U_S|\phi\rangle$ and $|\phi\rangle$ in terms of θ and φ.







Solution



After an application of the Grover operator, the angle between $U_\Psi U_S|\phi\rangle$ and $|\phi\rangle$ is 2φ, and the angle between $U_\Psi U_S|\phi\rangle$ and $|S\rangle$ is $\theta - 2\varphi$.

1 P. (d) Give the value of the angle φ in the previous question in terms of M and N

Solution

From the drawing, we have that $\cos\varphi = |\langle\Psi^\perp|S\rangle|$ and $\sin\varphi = |\langle\Psi|S\rangle|$. The second is easy to compute and gives $|\langle\Psi|S\rangle| = \sqrt{\frac{M}{N}}$. Then we have $\varphi = \arcsin\sqrt{\frac{M}{N}}$.

2 P. (e) Just as in the case of a single marked element, the operator G rotates the state by a certain angle, such that

$$\theta^{(k)} = \theta^{(k-1)} - 2\varphi\,.$$

We now want to find the number of steps necessary for the k-th iteration $|\phi^k\rangle$ to be close to $|S\rangle$. Identify such a k.

Hint: Remember that the algorithm is initialized in $|\Psi\rangle$. You can also use the fact that $\arcsin x \approx x$ for small x to obtain the scaling mentionned in the script.

Solution

We have that $\theta^{(k)} = \theta^{(0)} - 2k\varphi$. From the previous question, we also know that $\sin\varphi = |\langle\Psi|S\rangle| = \sqrt{\frac{M}{N}}$. At the beginning of the algorithm, the state is initialized to $|\Psi\rangle$, so $\theta^{(0)} = \frac{\pi}{2} - \varphi$ (see the figures above). Putting things together, we have that

$$\theta^{(k)} = \frac{\pi}{2} - (2k+1)\arcsin\left(\sqrt{\frac{M}{N}}\right)$$

and we want $\theta^{(k)} \approx 0$, so

$$k \approx \frac{\pi}{4\arcsin\left(\sqrt{M/N}\right)} - \frac{1}{2}$$

Using the assumption that $N \gg M$ we can approximate $\arcsin\left(\sqrt{M/N}\right) \approx \sqrt{M/N}$ and obtain

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}} - \frac{1}{2} - O\left(\sqrt{\frac{M}{N}}\right)$$

1 P. (f) After the adequate number of steps one reaches $|\phi^k\rangle \approx |S\rangle$. The last thing to do is to measure in the computational basis. Will a single measurement allow to know all marked elements? Motivate your answer.

Solution

Let us assume that after the optimal number of steps the state is exactly the target state $|\phi^k\rangle = |S\rangle$ (it will not be the case, but it is helpful for the sake of the argument). Measuring in the computational basis corresponds to the projective measurement where the projectors are $\Pi_x = |x\rangle\langle x|$ for $x = 0, \ldots, N-1$. Then, for a specific basis state x^*,

$$\Pi_{x^*}|S\rangle = |x^*\rangle\langle x^*|\frac{1}{\sqrt{M}}\sum_{x\in S}|x\rangle = \begin{cases} \frac{1}{\sqrt{M}}|x^*\rangle & \text{if } x^* \in S \\ 0 & \text{else.} \end{cases}$$

We obtain that a projective basis measurement will return one of the marked elements with equal probability. That is sufficient if one wants to find one of the marked elements, otherwise the procedure has to be repeated.

Recap

This exercise builds directly on top of the bonus exercise in Sheet 9. This time, instead of talking about states, we want to shift our attention towards channels. For this exercise, we adopt the definitions from the recap exercise of the previous sheet:

- Let $\mathcal{H}_A, \mathcal{H}_B$ be two d-dimensional Hilbert spaces.
- The *Othonormal basis of unitaries* of a d-dimensional Hilbert space is $\{U_j \mid j \in \{1, \ldots, d^2\}\}$.
- Let $|\omega\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be a maximally entangled state $|\omega\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$.
- Let $\mathcal{B}$ be an *orthonormal basis of maximally entangled states*: $\mathcal{B} := \{|\psi_j\rangle = (\mathbb{I}\otimes U_j)|\omega\rangle \mid j \in \{1, \ldots, d^2\}\}$.
- Let $p = (p_j)_{j=1}^{d^2}$ be a discrete probability distribution: $p_j \in [0,1]$, $\sum_j p_j = 1$.

11 P. **Bonus Exercise 2.** Consider the following quantum channel $\mathcal{N}_p$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$:

$$\mathcal{N}_p[\rho] = \sum_{j=1}^{d^2} p_j (\mathbb{I} \otimes U_j)\rho(\mathbb{I} \otimes U_j)^\dagger . \tag{1}$$

And consider again a maximally entangled quantum state $\Omega = |\omega\rangle\langle\omega|$.

1 P. (a) Find a p for which $\mathcal{N}_p$ is a unitary channel.

Hint: Pick the simplest p you can, so that you can prove the desired property in a few lines.

Solution

Since the Kraus operators of the channel are rescaled unitary operations, choosing $p = \delta_k$ for some value of $k \in \{1, \dots, d^2\}$ will result in the channel being

$$\mathcal{N}_p[\rho] = (\mathbb{I} \otimes U_k)\rho(\mathbb{I} \otimes U_k)^\dagger$$

which is unitary.

1 P. (b) Consider a p which is obtained from first sampling d numbers uniformly at random from $[0, 1]$, and then normalizing appropriately. Do you expect $\mathcal{N}_p$ to be unitary?

Solution

The channel $\mathcal{N}_p$ is unitary only if the distribution p is a delta function. As a consequence, there are finitely many choices of p for which the channel is unitary. In contrast, there are infinitely many choices for p that are not the delta function, thus the channel not being unitary. In more mathematical terms, the probability of the channel being unitary is zero

$$\begin{aligned}\mathbb{P}[\mathcal{N}_p \text{ is unitary}] &= \mathbb{P}[\exists 1 \le k \le d^2 : p = \delta_k] \\ &\le \sum_{k=1}^{d^2} \mathbb{P}[p = \delta_k] \\ &= 0\,,\end{aligned}$$

Here, the last step is due to the fact that p can be described by a continuous probability density function. Any random realization of p has then probability zero. This is in particular true for uniformly random p.

1 P. (c) Compute $\mathcal{N}_p[\Omega]$. Have we seen it before (e.g., on the last sheet)?

Solution

$$\begin{aligned}\mathcal{N}_p[\Omega] &= \sum_{j=1}^{d^2} p_j (\mathbb{I} \otimes U_j)|\omega\rangle\langle\omega|(\mathbb{I} \otimes U_j)^\dagger \\ &= \sum_{j=1}^{d^2} p_j |\psi_j\rangle\langle\psi_j| = \rho_p\,.\end{aligned}$$

This channel is constructed such that applying it to the maximally entangled state gives ρ_p from Bonus Exercise 1 of Sheet 9. Note: Here, the channel acts on the composite Hilbert space that the maximally entangled state lives in.

3 P. (d) Given a sufficiently large third Hilbert space $\mathcal{H}_C$ give an isometry $V_p : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ such that

$$\mathrm{Tr}_C(V_p \rho_{AB} V_p^\dagger) = \mathcal{N}_p[\rho_{AB}].$$

Hint: For our purposes, an isometry is a matrix V_p such that $V_p^\dagger V_p = \mathbb{I}_A \otimes \mathbb{I}_B$. Careful, in contrast with unitaries where $U^\dagger U = UU^\dagger$, it is not true here.

Solution

Let us define

$$V_p = \sum_j \sqrt{p_j}(\mathbb{I} \otimes U_j \otimes |j\rangle)$$

Then

$$\begin{aligned} V_p \sigma V_p^\dagger &= \sum_{j,j'} \sqrt{p_j}\sqrt{p_{j'}}(\mathbb{I} \otimes U_j \otimes |j\rangle)\rho_{AB}(\mathbb{I} \otimes U_{j'}^\dagger \otimes \langle j'|) \\ &= \sum_{j,j'} \sqrt{p_j}\sqrt{p_{j'}}(\mathbb{I} \otimes U_j)\rho_{AB}(\mathbb{I} \otimes U_{j'}^\dagger) \otimes |j\rangle\langle j'|) \,. \end{aligned}$$

Tracing out the third subsystem leaves

$$\begin{aligned} \mathrm{Tr}_C[V_p \sigma V_p^\dagger] &= \mathrm{Tr}_C \left[\sum_{j,j'} \sqrt{p_j}\sqrt{p_{j'}}(\mathbb{I} \otimes U_j)\rho_{AB}(\mathbb{I} \otimes U_{j'}^\dagger) \otimes |j\rangle\langle j'|) \right] \\ &= \sum_{j,j'} \sqrt{p_j}\sqrt{p_{j'}}(\mathbb{I} \otimes U_j)\rho_{AB}(\mathbb{I} \otimes U_{j'}^\dagger)\delta_{j,j'} \\ &= \sum_j p_j(\mathbb{I} \otimes U_j)\rho_{AB}(\mathbb{I} \otimes U_j^\dagger) \\ &= \mathcal{N}_p[\rho_{AB}] \,. \end{aligned}$$

We just built the Stinespring isometry from the Kraus decomposition of the channel. We could extend the isometry V_p to be unitary U_p, like in the script, for a certain auxiliary state η such that

$$\mathcal{N}_p[\rho_{AB}] = \mathrm{Tr}_C[U_p(\rho_{AB} \otimes \eta_C)U_p^\dagger]$$

but it would be somewhat more involved.

1 P. (e) Write down a set of Kraus operators for $\mathcal{N}_p$. Prove that the set you wrote down is actually a valid set of Kraus operators and that it represents $\mathcal{N}_p$.

Solution

From Eq. (1), it is straightforward to read off the Kraus operators $\{\sqrt{p_j}(\mathbb{I}\otimes U_j)\}_{j=1}^{d^2}$. To check that they are trace preserving, thus valid Kraus operators, we just compute

$$\begin{aligned}\sum_{j=1}^{d^2}\left(\sqrt{p_j}(\mathbb{I}\otimes U_j)\right)^\dagger\sqrt{p_j}(\mathbb{I}\otimes U_j) &= \sum_{j=1}^{d^2} p_j\mathbb{I}\otimes\underbrace{U_j^\dagger U_j}_{=\mathbb{I}}\\ &= \underbrace{\left(\sum_{j=1}^{d^2} p_j\right)}_{=1}\mathbb{I}\otimes\mathbb{I}\\ &= \mathbb{I}\otimes\mathbb{I}\,.\end{aligned}$$

3 P. (f) The unitarity of a channel can be defined as the purity of its corresponding Choi state. Compute the unitarity of $\mathcal{N}_p$, for an arbitrary given p. Compute the Choi rank of $\mathcal{N}_p$. *Careful! $\mathcal{N}_p$ as a channel acts on $\mathcal{H}_A\otimes\mathcal{H}_B$. In order to find the Choi state, you need to consider a maximally entangled state between two copies of $\mathcal{H}_A\otimes\mathcal{H}_B$: $|\tilde{\omega}\rangle\in(\mathcal{H}_A\otimes\mathcal{H}_B)^{\otimes 2}$. This would be, for example $|\tilde{\omega}\rangle=\frac{1}{d}\sum_{i,j=0}^{d-1}|ij\rangle\otimes|ij\rangle$. This is slightly different from what we are used to seeing, so proceed with care, one step at a time.*

Solution

Version 1: direct computation.

We compute first the Choi-state, and then evaluate the required quantities from it. By definition, $\mathcal{N}_p$ acts on $\mathcal{H}_A \otimes \mathcal{H}_B$, so in order to compute the Choi state, we need to consider another copy of this tensor product space. In total, we will have the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A \otimes \mathcal{H}_B$.

The next thing we need is to consider the density matrix of the new, larger, maximally entangled state:

$$\begin{aligned}\tilde{\Omega} &= |\tilde{\omega}\rangle\langle\tilde{\omega}| && (2)\\ &= \left(\frac{1}{d}\sum_{ij}|ij\rangle \otimes |ij\rangle\right)\left(\frac{1}{d}\sum_{kl}\langle kl| \otimes \langle kl|\right) && (3)\\ &= \frac{1}{d^2}\sum_{ijkl}|ijij\rangle\langle klkl|. && (4)\end{aligned}$$

We are dealing with 4-indexed kets and bras, so we need to be careful. We next do a small trick in which we re-order the indices that correspond to each of the subsystems. To be clear, $|\tilde{\omega}\rangle$ the way we wrote it now is a maximally entangled state living in $(\mathcal{H}_A \otimes \mathcal{H}_B) \otimes (\mathcal{H}_A \otimes \mathcal{H}_B)$. The parenthesis indicate the "cut" across which we consider the entanglement. We did not dwell on why this is important before, but recall that we have always talked about entanglement in the context of *bipartite systems*. In this exercise we are dealing with 4 different Hilbert spaces, which we group into two parts, as indicated by the parenthesis. In the following, we refer to the four Hilbert spaces with the subscripts A_1, B_1, A_2, and B_2, respectively. That being said, let us expand the kets and bras into all their tensor factors, and then re-group them differently:

$$\begin{aligned}\tilde{\Omega} &= \frac{1}{d^2}\sum_{ijkl}|ijij\rangle\langle klkl| && (5)\\ &= \frac{1}{d^2}\sum_{ijkl}\left(|i\rangle_{A_1}|j\rangle_{B_1}|i\rangle_{A_2}|j\rangle_{B_2}\right)\left(\langle k|_{A_1}\langle l|_{B_1}\langle k|_{A_2}\langle l|_{B_2}\right) && (6)\\ &= \frac{1}{d^2}\sum_{ijkl}|i\rangle\langle k|_{A_1} \otimes |j\rangle\langle l|_{B_1} \otimes |i\rangle\langle k|_{A_2} \otimes |j\rangle\langle l|_{B_2} && (7)\\ &= \frac{1}{d^2}\sum_{ijkl}|i\rangle\langle k|_{A_1} \otimes |i\rangle\langle k|_{A_2} \otimes |j\rangle\langle l|_{B_1} \otimes |j\rangle\langle l|_{B_2} && (8)\\ &= \frac{1}{d^2}\sum_{ijkl}|ii\rangle\langle kk|_{A_1A_2} \otimes |jj\rangle\langle ll|_{B_1B_2} && (9)\\ &= \left(\frac{1}{d}\sum_{ik}|ii\rangle\langle kk|_{A_1A_2}\right) \otimes \left(\frac{1}{d}\sum_{jl}|jj\rangle\langle ll|_{B_1B_2}\right) && (10)\\ &= \Omega_{A_1A_2} \otimes \Omega_{B_1B_2}. && (11)\end{aligned}$$

This might be surprising[a]: the maximally entangled state across the $(1,2)$ cut is a product state across the (A,B) cut. Indeed, we see that $\tilde{\Omega}$ is the tensor product of two maximally entangled states, one between both copies of $\mathcal{H}_A$, and one between both copies of $\mathcal{H}_B$. This will be useful in the next step.

[a] For some intuition, you can look at this object in graphical notation.

Solution

Next we must apply a channel on $\tilde{\Omega}$, and namely $\mathbb{I}\otimes\mathcal{N}_p$: which corresponds to doing nothing on the first copy of the Hilbert space, and applying $\mathcal{N}_p$ on the second one. Let us also expand this new channel out in the four tensor product indices. For each of the orthonormal basis of unitaries U_k, we introduce the curly notation $\mathcal{U}_j$ for the unitary channels $\mathcal{U}_j[\rho_B] = U_j \rho_B U_j^\dagger$.

$$\begin{aligned}
(\mathbb{I}_{A_1B_1} \otimes \mathcal{N}_p)\,[\tilde{\Omega}] &= \left(\mathbb{I}_{A_1} \otimes \mathbb{I}_{B_1} \otimes \mathbb{I}_{A_2} \otimes \left(\sum_j p_j \mathcal{U}_j \right)_{B_2} \right) [\tilde{\Omega}] && (12)\\
&= \left(\mathbb{I}_{A_1} \otimes \mathbb{I}_{B_1} \otimes \mathbb{I}_{A_2} \otimes \left(\sum_j p_j \mathcal{U}_j \right)_{B_2} \right) [\Omega_{A_1A_2} \otimes \Omega_{B_1B_2}] && (13)\\
&= (\mathbb{I}_{A_1} \otimes \mathbb{I}_{A_2})[\Omega_{A_1A_2}] \otimes \left(\mathbb{I}_{B_1} \otimes \left(\sum_j p_j \mathcal{U}_j \right)_{B_2} \right) [\Omega_{B_1B_2}] && (14)\\
&= \Omega_{A_1A_2} \otimes \sum_j p_j (\mathbb{I} \otimes U_j) \Omega_{B_1B_2} (\mathbb{I} \otimes U_j)^\dagger && (15)\\
&= \Omega_{A_1A_2} \otimes (\rho_p)_{B_1B_2}\,, && (16)
\end{aligned}$$

where ρ_p was defined in question (c). What we did was use the re-writing of the maximally entangled state as a product to show that the Choi state is a tensor product between the maximally entangled state on the two copies of $\mathcal{H}_A$ and the channel $\mathcal{N}_p$ applied on the two copies of $\mathcal{H}_B$.

Since $\mathcal{N}_p[\rho_{AB}] = (\mathbb{I} \otimes \mathcal{M}_p)[\rho_{AB}]$ for the channel $\mathcal{M}$ given by the unitaries, in the end, it is a local operation (only on system B). From this one can be less surprised that the Choi operator on AB is a product state.

With this, we have found the Choi state of $\mathcal{N}_p$. From here, we can directly compute the unitarity and the Choi rank of the channel by computing the purity and the rank of the state. We do not need to use any formulas, we just port the results from Sheet 9. The Choi state being a product state between the pure maximally entangled state Ω and the state ρ_p from sheet 9, it follows that:

- The purity of the Choi state is the purity of ρ_p, which we know is $\sum_j p_j^2$, or, said otherwise, the variance of the distribution p.
- The rank of the Choi state is the rank of ρ_p, which we know is equal to the number of non-zero entries of p.

Solution

Version 2: using that the channel is separable.

In this version, we reach the same results but using some information from the channel to reduce some of the calculation. Starting from the hint, we can rewrite the maximally entangled state

$$\begin{aligned}
|\tilde{\omega}\rangle &= \frac{1}{d}\sum_{i,j=0}^{d-1} |ij\rangle_{A_1B_1} \otimes |ij\rangle_{A_2B_2} \\
&= \frac{1}{d}\sum_{i,j=0}^{d-1} |i\rangle_{A_1} \otimes |j\rangle_{A_2} \otimes |j\rangle_{B_1} \otimes |j\rangle_{B_2} \\
&= \left(\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1} |i\rangle_{A_1} \otimes |j\rangle_{A_2}\right)\left(\frac{1}{\sqrt{d}} \otimes |j\rangle_{B_1} \otimes |j\rangle_{B_2}\right) \\
&= |\omega\rangle_{A_1A_2} \otimes |\omega\rangle_{B_1B_2} \,.
\end{aligned}$$

Then, the density matrix is given by $\tilde{\Omega} = |\tilde{\omega}\rangle\langle\tilde{\omega}| = \Omega_{A_1A_2} \otimes \Omega_{B_1B_2}$. Then to compute the Choi state, observe that the channel of interest is separable, and we have that

$$\mathcal{N}_p[\rho] = \left(\mathcal{I}^{(A)} \otimes \mathcal{M}_p^{(B)}\right)[\rho]$$

where $\mathcal{I}^{(A)}$ and $\mathcal{M}_p^{(B)}$ are local quantum channels, with Kraus operators $\{\mathbb{I}\}$ and $\{\sqrt{p_j}U_j\}$ respectively

$$\begin{aligned}
\mathcal{I}^{(A)}[\rho] &= \rho \\
\mathcal{M}_p^{(B)}[\rho] &= \sum_{j=1}^{d^2} p_j U_j \rho U_j^\dagger \,.
\end{aligned}$$

Putting things together, we can separate the action of the two channels on the respective maximally entangled states

$$\begin{aligned}
J(\mathcal{N}_p) &= \left(\mathbb{I}_{A_1B_1} \otimes \mathcal{N}_p\right)[\tilde{\Omega}_{A_1B_1A_2B_2}] \\
&= \left(\mathbb{I}_{A_1} \otimes \mathbb{I}_{B_1} \otimes \mathcal{I}^{(A)} \otimes \mathcal{M}_p^{(B)}\right)[\Omega_{A_1A_2} \otimes \Omega_{B_1B_2}] \\
&= \left(\mathbb{I}_{A_1} \otimes \mathcal{I}^{(A)}\right)[\Omega_{A_1A_2}] \otimes \left(\mathbb{I}_{B_1} \otimes \mathcal{M}_p^{(B)}\right)[\Omega_{B_1B_2}] \\
&= \Omega_{A_1A_2} \otimes \sum_j p_j (\mathbb{I} \otimes U_j)\Omega_{B_1B_2}(\mathbb{I} \otimes U_j)^\dagger \\
&= \Omega_{A_1A_2} \otimes (\rho_p)_{B_1B_2} \\
&= J(\mathcal{I}^{(A)}) \otimes J(\mathcal{M}_p^{(B)})
\end{aligned}$$

1 P. (g) Find a channel for which $\mathcal{N}_p[\Omega]$ is the Choi state.

Solution

From the previous question, we already have that $\mathcal{N}_p[\Omega] = \rho_p = J(\mathcal{M}_p^{(B)})$. Let us make this observation explicit again. By definition, for some channel

$$T(\rho) = \sum_k E_k \rho E_k^\dagger$$

the Choi state is the result of applying that channel to one half of a maximally entangled state with a second (auxiliary) system of the same size

$$J(T) = (\mathbb{I} \otimes T)(\Omega) = \sum_k (\mathbb{I} \otimes E_k)\Omega(\mathbb{I} \otimes E_k^\dagger).$$

This is exactly $\mathcal{N}_p[\Omega]$ if we choose $E_k = \sqrt{p_k} U_k$. So $\mathcal{N}_p[\Omega]$ is the Choi state of the channel whose Kraus decomposition is

$$\mathcal{M}_p^{(B)}(\rho) = \sum_j p_j U_j \rho U_j^\dagger.$$

Total Points: 17 (+14)