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 $|x\rangle \otimes |-\rangle$?

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 $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{y \cdot x} = \delta_{y,0^n}$.

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)?

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 $2^{n-\ell}$.

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.

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

$$\begin{aligned} &\text{uniform superposition} && |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \\ &\text{marked superposition} && |S\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle \,. \end{aligned}$$

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 $\text{span}\{|\Psi\rangle, |S\rangle\}$.

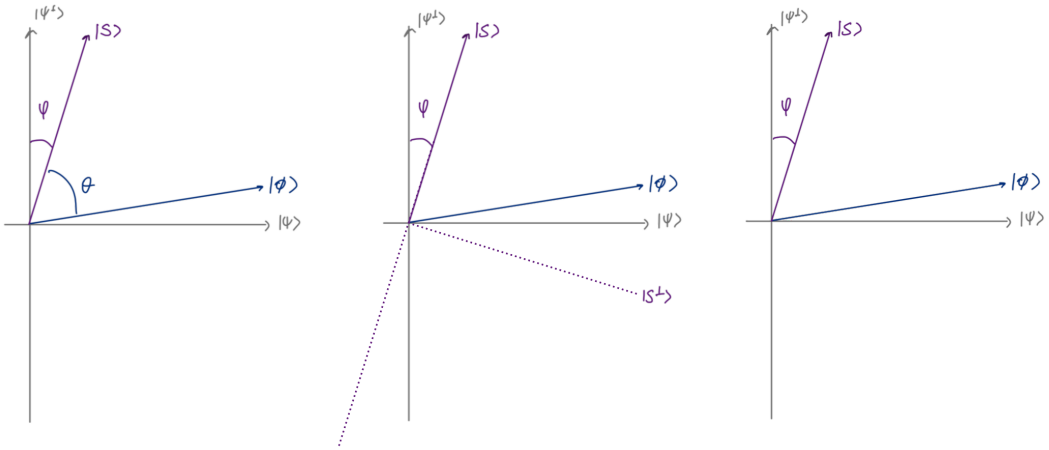
Hint: Look at the effect of U_S and U_Ψ on both $|\Psi\rangle$ and $|S\rangle$.

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

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

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

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.



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

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.

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 $\{U_j \,|\, j \in \{1, \ldots, d^2\}\}$.
- 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*: $\mathcal{B} \coloneqq \{|\psi_j\rangle = (\mathbb{I} \otimes U_j)|\omega\rangle \,|\, j \in \{1, \ldots, d^2\}\}$.
- 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.

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?

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

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.

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 $\mathcal{N}_p$.

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.*

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

Total Points: 17 (+14)