2021 Quantum Computing Homework Nr. 8

András Gilyén

November 5, 2021

Homework exercises – second extended edition – you can earn 15 points in total as opposed to the usual 10 points! Each exercise is worth one more point than its number except exercise 2 which is worth 4. On the last page you can find some hints where indicated by (**H**).

Reminder

Recall the *Spectral Theorem* (*Főtengely Tétel in Hungarian*): for every self-adjoint matrix $A \in \mathbb{C}^{d\times d}$ there exists a unitary $V \in \mathbb{C}^{d\times d}$ that diagonalizes A, i.e., $A = V \cdot D \cdot V^\dagger$ where $D \in \mathbb{R}^{d\times d}$ is a diagonal matrix containing the eigenvalues of A, and the columns of V are the corresponding eigenvectors. Let $|v_i\rangle$ be the i-th column of V and let λ_i be the i-th diagonal entry of D. In Dirac notation we can write $A = \sum_{i=0}^{d-1} \lambda_i |v_i\rangle\langle v_i|$.

Recall a generalization of the Spectral Theorem for arbitrary matrices, called *Singular Value Decomposition*: for every matrix $A \in \mathbb{C}^{d\times k}$ there exists unitaries $V \in \mathbb{C}^{d\times d}$, $W \in \mathbb{C}^{k\times k}$ and a diagonal matrix $\Sigma \in \mathbb{R}_{\geq 0}^{d\times k}$ containing the singular values on the diagonal such that $A = V \cdot \Sigma \cdot W^\dagger$. The columns v_i of V are called the left singular vectors and the columns w_i of W are called the right singular vectors of A. Let σ_i be the i-th diagonal entry of Σ, then in Dirac notation we can write $A = \sum_{i=0}^{d-1} \sigma_i |v_i\rangle\langle w_i|$.

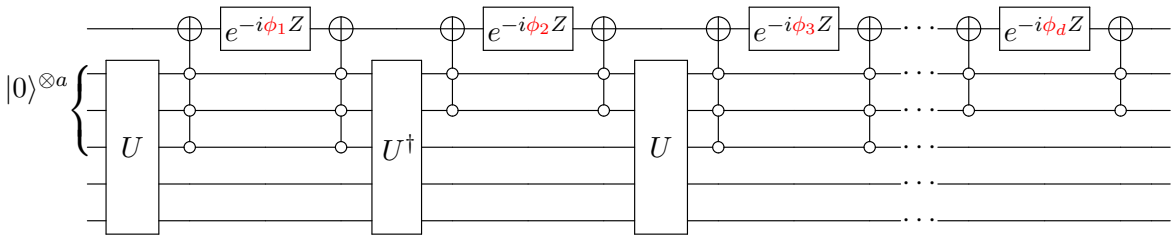
We say that a polynomial $p(x)$ is even/odd if it is an even/odd function of x or equivalently if its coefficients are non-zero only for even/odd powers of x.

Theorem 1 (Quantum Singular Value Transformation (QSVT); G, Su, Low, Wiebe 2018)**.** *Let $P\colon [-1,1] \mapsto [-1,1]$ be a degree-d even/odd polynomial map. Suppose that U is a block-encoding of $A = (\langle 0^a| \otimes I)U(|0^b\rangle \otimes I)$ that has singular value decomposition $A = V\Sigma W^\dagger$. Then $Q := (H \otimes I)U_\Phi(H \otimes I)$ is a block-encoding of*

$$VP(\Sigma)W^\dagger = (\langle 0^{a+1}| \otimes I)Q(|0^{b+1}\rangle \otimes I) \quad \text{if } d \text{ is odd, and} \tag{1}$$

$$WP(\Sigma)W^\dagger = (\langle 0^{a+1}| \otimes I)Q(|0^{b+1}\rangle \otimes I) \quad \text{if } d \text{ is even,} \tag{2}$$

where $\Phi \in \mathbb{R}^d$ is efficiently computable from P and U_Φ is the following circuit:[*]



(In the even case $P(\Sigma)$ should be interpreted as a $k \times k$ matrix, where the j-th diagonal entry is $P(\sigma_j)$, where σ_j is defined as 0 for $j \geq \max\{d,k\}$.)

[*]The empty dots denote control on the state $|0\rangle$. The generalized $CNOT$/Toffoli gates are controlled by $|0^a\rangle$ and $|0^b\rangle$ on the right- and left-hand sides of U respectively in the circuit – in this example circuit $a = 3$, $b = 2$, and d is even.

Exercises

1.) Linear combination of unitaries: Suppose that $A_0 = (\langle 0^a| \otimes I)U_0(|0^b\rangle \otimes I)$ and $A_1 = (\langle 0^a| \otimes I)U_1(|0^b\rangle \otimes I)$. Given $\alpha_0, \alpha_1 \in \mathbb{C}$ such that $|\alpha_0| + |\alpha_1| = 1$, construct a circuit that uses $U = |0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1$ and two single qubit gates to implement a block-encoding V of $\alpha_0 A_0 + \alpha_1 A_1$ such that

$$(\langle 0^{a+1}| \otimes I)V(|0^{b+1}\rangle \otimes I) = \alpha_0 A_0 + \alpha_1 A_1. \qquad (\mathbf{H})$$

2.) From Ronald's lecture notes [dW19, Chapter 9 Exercise 8]: Block-encoding an s-sparse Hermitian matrix A with $\|A\| \leq 1$ (see Section 9.4). Assume for simplicity that the entries of A are real.

(a) Show how to implement W_1 using an $O_{A,loc}$-query and a few other A-independent gates. For simplicity you may assume s is a power of 2 here, and you can use arbitrary single-qubit gates, possibly controlled by another qubit.
(Note that the same method allows to implement W_3.)

(b) Show how to implement W_2 using an O_A-query, an O_A^{-1}-query, and a few other A-independent gates (you may use auxiliary qubits as long as those start and end in $|0\rangle$). Note that W_2 just implements a rotation on the first qubit, by an angle that depends on A_{kj}. There's no need to write out circuits fully down to the gate-level here; it suffices if you describe the idea precisely.

(c) Show that the $(0^{n+1}i, 0^{n+1}j)$-entry of $W_3^{-1}W_1$ is $1/s$ if $A_{ij} \neq 0$, and is 0 if $A_{ij} = 0$.

(d) Show that the $(0^{n+1}i, 0^{n+1}j)$-entry of $W_3^{-1}W_2W_1$ is exactly A_{ij}/s.

3.) This exercise shows that singular value transformation is a generalization of eigenvalue transformation just as singular value decomposition is a generalization of the spectral decomposition.

(a) Prove that for a Hermitian matrix A and an even or odd polynomial P the expressions (2) or (1) respectively coincide with $P(A)$. (**H**)

(b) Prove that for every polynomial $P\colon [-1,1] \mapsto [-\frac{1}{2}, \frac{1}{2}]$ there is a quantum circuit that uses a (controlled) block-encoding U (or its inverse $U^\dagger$) of a Hermitian matrix A a total of $\mathcal{O}(\deg(P))$ times and implements a block-encoding of $P(A)$. (**H**)

4.) This exercise shows some applications of QSVT. You may use results form the above exercises.

(a) (Fixed-point) Amplitude Amplification:[†] Suppose U is a quantum circuit that prepares some n-qubit state $|\psi\rangle$, i.e., $U\colon |0^n\rangle \mapsto |\psi\rangle = \sqrt{p'}|0\rangle|G\rangle + \sqrt{1-p'}|1\rangle|B\rangle$, where $|G\rangle$ and $|B\rangle$ are some $(n-1)$-qubit pure states and $p' > p$ for some known p. Give an algorithm using QSVT that outputs the state $|G\rangle$ with success probability at least $1-\varepsilon$ and uses U and $U^\dagger$ a total of $\mathcal{O}\Big(\frac{\log(1/\varepsilon)}{\sqrt{p}}\Big)$ times. (**H**)

(b) Oblivious Amplitude Amplification:[‡] Suppose U is a quantum circuit that is a block-encoding of a subnormlized unitary V such that $\frac{1}{2}V = (\langle 0^a| \otimes I)U(|0^a\rangle \otimes I)$. Using QSVT implement the unitary V with 3 uses of U or $U^\dagger$. (**H**)

(c) Using the Taylor series $e^{itx} = \sum_{k=0}^{\infty} \frac{(itx)^k}{k!}$ give a polynomial approximation $P(x)$ of degree $\mathcal{O}(|t| + \log(1/\varepsilon))$ such that $|P(x) - e^{itx}| \leq \varepsilon$ and $|P(x)| \leq 1$ for all $x \in [-1,1]$. (**H**)

(d) Suppose U is a block-encoding of the Hermitian matrix H. Give a block-encoding of an ε-approximation of $e^{itH}/2$ that uses U and $U^\dagger$ a total of $\mathcal{O}(|t| + \log(1/\varepsilon))$ times. (**H**)

(e) Sparse Hamiltonian Simulation: Suppose the Hamiltonian is s-sparse and we have sparse-access to it as in Exercise 2. Give an algorithm that implements e^{itH} with ε accuracy using $\mathcal{O}(s|t| + \log(1/\varepsilon))$ queries to the "sparse access" oracles. It suffices to argue on a high level.

[†]Note that this is slightly more general than the amplitude amplification problem from last week where we required knowledge of p; the name "fixed-point" vaguely refers to this (and to some history of related algorithms).

[‡]This is a generalization of amplitude amplification, which works for several input states simultaneously, hence the name "oblivious". In fact this also works if V is only an isometry and $\frac{1}{2}V = (\langle 0^a| \otimes I)U(|0^b\rangle \otimes I)$ where $b \geq a$.

Hints

Exercise 1: Remember from the lecture that $(\langle 0^{a+1}| \otimes I)(H \otimes I)U(H \otimes I)(|0^{b+1}\rangle \otimes I) = \frac{1}{2}(A_0 + A_1)$. Replace the Hadamrd gates with appropriate single-qubit gates.

Exercise 3a: You may use the fact that the matrices in (1)-(2) are well defined in the sense that they define the same matrix independent of the particular choice of singular value decomposition. (The singular value decomposition is not necessarily unique.) Then "convert" and eigenvalue decomposition of A to a singular value decomposition.

Exercise 3b: Decompose P into even/odd parts.

Exercise 4a: You may use the fact that for every $t \in (0,1)$ there are even/odd polynomials $P\colon [-1,1] \mapsto [-1,1]$ of degree $\mathcal{O}\left(\frac{\log(1/\varepsilon)}{t}\right)$ such that $P(x) \geq 1 - \varepsilon$ for every $x \in [t,1]$.

Exercise 4b: Consider using a Chebyshev polynomial. Do you notice some similarity with [dW19, Chapter 7 Exercise 1]?

Exercise 4c: You may use that by Striling's approximation $k! \geq (k/e)^k$.

Exercise 4d: Observe that $e^{itx} = i\sin(tx) + \cos(tx)$.

References

[dW19] Ronald de Wolf. Quantum computing: Lecture notes, 2019. arXiv: 1907.09415