Problem Set 2: Proving the QSVT

July 25, 2023

Problem 1 (When will my reflection show who I am inside?)**.** QSVT achieves polynomials by interspersing phase operators with signal rotation operators. However, these rotation operators may look different in the literature. Consider two potential operators, $W(x), R(x)$, with the following matrix forms:

$$W(x) = \begin{pmatrix} x & i\sqrt{1-x^2} \\ i\sqrt{1-x^2} & x \end{pmatrix} \qquad R(x) = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \tag{1}$$

Where W is the rotation operator while R is the reflection operator. We can define two different kinds of QSP, $\mathbf{QSP}_W(\Phi, x)$ and $\mathbf{QSP}_R(\Phi, x)$ for these two different operators. For example,

$$\mathbf{QSP}_W(\Phi, x) \coloneqq \Big(\prod_{j=1}^{n} e^{\mathrm{i}\phi_j \sigma_z} W(x) \Big) e^{\mathrm{i}\phi_0 \sigma_z}.$$

Suppose we have some series of phases $\Phi = (\phi_0, \ldots, \phi_n)$ such that $\mathbf{QSP}_W(\Phi, x)$ forms a desired polynomial $p(x)$. Can we find a Φ' such that $\mathbf{QSP}_R(\Phi', x)$ performs the same polynomial? If so, find a formula for Φ' in terms of Φ; if not, prove why.

Solution. (From [MRTC21, Appendix A.2]) We can notice that

$$\begin{aligned} W(x) &= \begin{pmatrix} 1 & \\ & i \end{pmatrix} \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \begin{pmatrix} 1 & \\ & i \end{pmatrix} \\ &= e^{\mathrm{i}\pi/2} \begin{pmatrix} e^{-\mathrm{i}\pi/4} & \\ & e^{\mathrm{i}\pi/4} \end{pmatrix} \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \begin{pmatrix} e^{-\mathrm{i}\pi/4} & \\ & e^{\mathrm{i}\pi/4} \end{pmatrix} \\ &= e^{\mathrm{i}\pi/2} e^{-\mathrm{i}\frac{\pi}{4}\sigma_z} R(x) e^{-\mathrm{i}\frac{\pi}{4}\sigma_z} \end{aligned}$$

So, if $\Phi = (\phi_0, \phi_1, \ldots, \phi_n)$ is the phase sequence for W, then $\Phi - (\pi/4, \pi/2, \pi/2, \ldots, \pi/2, \pi/4 - d\pi/2)$ is the phase sequence for R. $\square$

Problem 2 (Perfectly balanced, as all things should be)**.** The Chebyshev polynomials of the first and second kind are functions such that, for all $z \in \mathbb{C}$,

$$\begin{aligned} T_n(\tfrac{1}{2}(z + z^{-1})) &= \tfrac{1}{2}(z^n + z^{-n}) \\ U_n(\tfrac{1}{2}(z + z^{-1})) &= (z^{n+1} - z^{-(n+1)})/(z - z^{-1}) \end{aligned}$$

Prove that T_n and U_n are polynomials. Then, prove that

$$T_n(x)^2 + (1 - x^2) U_{n-1}(x)^2 = 1. \tag{2}$$

Just a little more and we have a proof that these can be used in QSP/QSVT!

Solution. $\square$

Problem 3 (They're the same picture!). Return to [BCCKS17, Lemma 3.6]. What are the angles of the phase operators? What are the polynomials that are being computed with these phase operators? (A recursive definition is fine.)

Solution. The key idea here is that the phase unitaries applied take the form $2\Pi - I$ for some projector Π. Thus, this is equivalent to performing a rotation of $\phi = \frac{\pi}{2}$. They are creating a Chebyshev polynomial taking $\sin\theta \mapsto \sin(2\ell+1)\theta$. $\square$

Problem 4 (Block-encodings for any matrix). Given a matrix $A \in \mathbb{C}^{d\times d}$ such that $\|A\| \leq 1$, show there exists a unitary $U \in \mathbb{C}^{2d\times 2d}$ such that U is a block-encoding of A:

$$U = \begin{pmatrix} A & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

Prove that $2d$ is tight, i.e., there is some matrix A such that any unitary with A as a submatrix must be size at least $2d \times 2d$. *Note: this is true for non-square A as well, but the argument might get more annoying.*

Solution. Consider the singular value decomposition $A = VDW^\dagger$. Then

$$\begin{pmatrix} V & \\ & I \end{pmatrix}\begin{pmatrix} D & \sqrt{1-D^2} \\ \sqrt{1-D^2} & -D \end{pmatrix}\begin{pmatrix} W^\dagger & \\ & I \end{pmatrix}$$

is a product of unitary matrices, where the top-left block is A. *For A non-square, this works via mimicking the structure CS decomposition.* If A is the zero matrix, then we need U to be size $2d \times 2d$; smaller matrices containing A must have linearly dependent columns.

(Alternative solution from [AA11, Lemma 29]) Since $A^\dagger A$ is a positive semi-definite matrix such that $\|A^\dagger A\| \leq 1$, then $I - A^\dagger A$ is also positive semi-definite, so it has a Hermitian square root $I - A^\dagger A = B^2 = B^\dagger B$. Since $A^\dagger A + B^\dagger B = I$,

$$\begin{pmatrix} A \\ B \end{pmatrix}^\dagger \begin{pmatrix} A \\ B \end{pmatrix} = I,$$

so this stacked $2d \times d$ matrix has orthonormal columns. Consequently, we can complete it to a $2d \times 2d$ unitary matrix. $\square$

Problem 5 (It's just a phase). In our QSVT algorithm, we needed to apply gates of the form $e^{i\phi(2\Pi - I)}$, where $\Pi = (|0\rangle^{\otimes a}\langle 0|^{\otimes a}) \otimes I$. How do you implement these?

Solution. A single ancilla coupled with Π-controlled nots are sufficient.

A Π-controlled not takes the following form:

$$C_\Pi NOT = \Pi \otimes X + (I - \Pi) \otimes I \tag{3}$$

So that $C_\Pi NOT e^{i\phi Z} C_\Pi NOT$ when applied to an ancilla of $|0\rangle$ is precisely the required circuit. (See [MRTC21] for more circuits). $\square$

References

[AA11] Scott Aaronson and Alex Arkhipov. "The computational complexity of linear optics". In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. ACM, June 2011. DOI: 10.1145/1993636.1993682. arXiv: 1011.3245 [quant-ph] (page 2).

[BCCKS17] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. "Exponential improvement in precision for simulating sparse hamiltonians". In: *Forum of Mathematics, Sigma* 5 (2017), e8. DOI: 10.1017/fms.2017.2. arXiv: 1312.1414 [quant-ph] (page 2).

[MRTC21] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. "Grand unification of quantum algorithms". In: *PRX Quantum* 2 (4 Dec. 2021), p. 040203. DOI: 10.1103/PRXQuantum.2.040203 (pages 1, 2).