Problem Set 1: The Block-Encoding

July 24, 2023

Problem 1 (Block-encodings: tensor products)**.** Let U and V be Q-block encodings of A and B, respectively. Show how to get a Q-block-encoding of $A \otimes B$.

Solution. $U \otimes V$ is a block-encoding of $A \otimes B$. □

Problem 2 (Extensibility properties)**.** Prove Corollary 1.8 of the lecture notes. Specifically, show that the two extensibility properties allow us to convert a Q-block encoding of A to a dQ-block encoding of $p^{(\mathrm{SV})}(A)$.

Solution. We can construct a kQ-block encoding of $m_k^{(\mathrm{SV})}(A)$, for $m_k(x) = x^k$. The problem here is that the naïve approach – producing x^d and then adding with x^{d-1} – would require $\mathcal{O}(d^2 Q)$ complexity.

Instead, via Horner's rule, we may rewrite the polynomial in the following form:

$$a_0 + x(a_1 + x(a_2 + ... + x(a_{n-1} + xa_n))) \tag{1}$$

Precisely the sum of products of polynomials. It can be shown that the coefficients can be structured carefully so that they never exceed 1. □

Solution. [Angus Lowe's solution] Consider the following preparation unitaries:

$$\mathrm{PREP}\,|0\rangle = \sum_k \sqrt{\lambda_k}\,|k\rangle \tag{2}$$

$$\mathrm{SELECT} = \sum_{k=0}^{d} |k\rangle\langle k| \otimes A^k \tag{3}$$

Then, the application of $\mathrm{PREP}^\dagger \cdot \mathrm{SELECT} \cdot \mathrm{PREP}$ precisely implements a desired block encoding with λ_k chosen appropriately. This is a version of linear combinations of unitaries seen in [Bab+18]. SELECT can be implemented efficiently via using a binary encoding in the ancilla and using $\log_2 d$ controlled-A^{2^j} gates. □

Problem 3 (Extensibility properties do not suffice)**.** Let $p(x) = \sum_{k=0}^{d} a_k x^k$ be a polynomial whose coefficients satisfy $\sum |a_k| \leq 1$. Show that $p(x)$ cannot approximate $\sin(100x)$ for any choice of d. That is, show that there is some $x \in [-1, 1]$ such that

$$|p(x) - \sin(100x)| \geq 0.01.$$

Solution. The key idea is straightforward: we want to show that any polynomial $p(x)$ has derivative $p'(x)$ that differs significantly from $\frac{d}{dx}\sin(100x)$ and use this to produce a contradiction.

First, consider $x = -\frac{\pi}{200}, x = \frac{\pi}{200}$. Then, $\sin(100x) = \pm 1$ at those points. Thus, by the Mean Value Theorem, p must at some point attain a derivative exceeding the following value:

$$\frac{0.99 - -0.99}{\frac{\pi}{200} - -\frac{\pi}{200}} = \frac{200 \cdot 0.99}{\pi} \geq 50 \tag{4}$$

Now, consider the maximum derivative attainable by the polynomial. Set $p(x) = \sum_{k=0}^{d} a_k x^k$ with $\sum |a_k| = 1$. Then,

$$\begin{aligned} |p'(x)| &\leq \left| \sum_{k=1}^{d} a_k \cdot k x^{k-1} \right| && (5)\\ &\leq \sum_{k=1}^{d} |a_k| k |x|^{k-1} && (6)\\ &\leq \sum_{k=1}^{d} k |x|^{k-1} && (7) \end{aligned}$$

Numerics can show that this function lies far below 50 for $x \in [\pm \frac{\pi}{200}]$.

Thus, for the polynomial to observe our requirements, it must attain a derivative of at least 50 at some point. However, on this interval, it has derivative far less. Thus, we have obtained a contradiction and p does not exist. □

Solution. [Zach's] Suppose we have a polynomial $p(x) = a_0 + \sum_{k=1}^{d} a_k x^k$. Then, because $|p(0)| \leq \frac{1}{100}$ by our constraint, we need $|a_0| \leq \frac{1}{100}$. Then, observe that, on $x \in [0, 1/2]$:

$$\begin{aligned} p(x) &\leq |a_0| + \sum_{k=1}^{d} |a_k| |x|^k && (8)\\ &\leq \frac{1}{100} + \frac{1}{2} && (9) \end{aligned}$$

Thus, the maximum attainable value of $p(x)$ is $\frac{51}{100}$. However, $x = \frac{\pi}{200}$ would mean $\sin(100x) = 1$, so $p(x)$ and $\sin(100x)$ differ from a quantity much greater than 0.01, a contradiction. □

Problem 4 (Oblivious amplitude amplification)**.** QSVT is a unifying technique which includes many major quantum algorithms, including amplitude amplification [MRTC21]. In this problem, we show that Oblivious Amplitude Amplification (OAA), as described in [BCCKS17, Lemma 3.6], can be written in our block-encoding framework.

Identify the block-encoding within the aforementioned unitary. What polynomial would effect the same transformation as described in [BCCKS17, Lemma 3.6]?

Solution. The state preparation unitary mentioned in [BCCKS17] performs the following transformation:

$$U |0\rangle^{\mu} |\psi\rangle = \sin\theta |0\rangle^{\mu} V |\psi\rangle + |\Phi^{\perp}\rangle \tag{10}$$

Where $|\Phi^\perp\rangle$ is an orthogonal component such that $\langle 0|^\mu \otimes I\, |\Phi^\perp\rangle = 0$. Then, U is a block-encoding of $\sin\theta V$, i.e.:

$$U = \begin{bmatrix} \sin\theta V & \cdot \\ \cdot & \cdot \end{bmatrix} \tag{11}$$

In fact, the net unitary we would like to implement is the following:

$$S^\ell U = \begin{bmatrix} \sin(2\ell+1)\theta V & \cdot \\ \cdot & \cdot \end{bmatrix} \tag{12}$$

Thus, we see that $S^\ell U$ actually implements a polynomial (Chebyshev polynomial) taking $\sin\theta$ to $\sin(2\ell+1)$. However, we need not use Chebyshev polynomials if we may tolerate a different construction. In particular, $\sin\theta$ will typically be known, so implementing any polynomial taking the specific value of $\sin\theta$ to $\sin(2\ell+1)\theta$ will suffice. □

Remark 1.1. See [Ral20] for more information on how to get block-encodings of density matrices and observables, and how to use this to estimate physical quantities like expectations of Gibbs states. See [BCCKS17] for further discussion of Hamiltonian simulation, placing it in the context of the more general problem of understanding the "fractional query model", "discrete query model", and "continuous query model". See [LC19] (the original paper) or [GSLW19] for a more thorough explanation of the Hamiltonian simulation algorithm.

References

[Bab+18] Ryan Babbush, Craig Gidney, Dominic W Berry, Nathan Wiebe, Jarrod McClean, Alexandru Paler, Austin Fowler, and Hartmut Neven. "Encoding electronic spectra in quantum circuits with linear T complexity". In: *Physical Review X* 8.4 (2018), p. 041015 (page 1).

[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] (pages 2, 3).

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. "Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics". In: *Proceedings of the 51st ACM Symposium on the Theory of Computing (STOC)*. ACM, June 2019, pp. 193–204. DOI: 10.1145/3313276.3316366. arXiv: 1806.01838 (page 3).

[LC19] Guang Hao Low and Isaac L. Chuang. "Hamiltonian simulation by qubitization". In: *Quantum* 3 (July 2019), p. 163. DOI: 10.22331/q-2019-07-12-163 (page 3).

[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 (page 2).

[Ral20] Patrick Rall. "Quantum algorithms for estimating physical quantities using block encodings". In: *Physical Review A* 102.2 (Aug. 2020), p. 022408. DOI: 10.1103/physreva.102.022408. arXiv: 2004.06832 [quant-ph] (page 3).