Quantum Linear Algebra Algorithms Tutorial

August 28, 2026

András Gilyén (Alfréd Rényi Institute of Mathematics)

Feel free to skip exercises that you find too easy, too hard, or less interesting. At page 4 you can find some hints where indicated by (**H**).

Exercises

1.) (**H**) Linear Combination of Unitaries:
Suppose that $U=\sum_i |i\rangle\langle i|\otimes U_i$, and $P:|0\rangle\mapsto\sum_i\sqrt{p_i}|i\rangle$ for $p_i\in[0,1]$.
Show that $(P^\dagger\otimes I)U(P\otimes I)$ is a block-encoding of the convex combination $\sum_i p_iU_i$.
In particular show that if $(\langle 0|\otimes I)U_i(|0\rangle\otimes I)=A_i$, then it is a block-encoding of

$$\sum_i p_iA_i.$$

How can you generalize this to linear combinations, e.g., add signs to some p_i?

2.) (**H**) Product of block-encoded unitaries:
Let $A,B\in\mathbb{C}^{2^m\times 2^m}$, and U_A, U_B block-encodings such that $A=(\langle 0^a|\otimes I)U_A(|0^a\rangle\otimes I)$, $B=(\langle 0^a|\otimes I)U_B(|0^a\rangle\otimes I)$. Construct an $(a+1)$-ancilla block-encoding of AB with a single use of U_A and U_B.

3.) (**H**) Szegedy walk as a block-encoding:
Let P be a symmetric (column) stochatic matrix, and consider the following coherent version of a step of a corresponding random walk:

$$U\colon |0\rangle|i\rangle\mapsto\sum_j\sqrt{P_{ji}}|j\rangle|i\rangle.$$

Show that $U^\dagger\cdot SWAP\cdot U$ is a block-encoding of P!

4.) Understanding singular value decompositions:

- **a.**) Let $A=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ and $B=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.
  - **i.**) What is the singular value decomposition of A?
  - **ii.**) Give a singular value decomposition of B!
  - **iii.**) What is the eigenvalue decomposition of B?
  - **iv.**) Give a singular value decomposition of B where the right singular vectors coincide with the eigenvectors!
- **b.**) Let $A=U^\dagger\Sigma V=\sum_{i=1}^m\sigma_i|u_i\rangle\langle v_i|$, where u_i,v_i are the columns of the unitaries U,V and $\sigma_1\geq\sigma_2\geq\ldots\geq\sigma_m\geq 0$ are the singular values of A. Prove that $A^\dagger A=\sum_{i=1}^m\sigma_i^2|v_i\rangle\langle v_i|$.
- **c.**) (**H**) We know that every Hermitian matrix $H\in\mathbb{C}^{n\times n}$ has a decomposition of the from $\sum_{i=1}^n\lambda_i|\psi_i\rangle\langle\psi_i|$, where $\lambda_i\in\mathbb{R}$ and $\langle\psi_i|\psi_j\rangle=\delta_{ij}$. Prove that every $A\in\mathbb{C}^{m\times n}$ has a singular value decomposition.

5.) (**H**) Prove the theorem below on Quantum Eigenvalue Transformation (QEVT):
Let $R \in \mathbb{C}^{N\times N}$ be a Hermitian unitary, i.e., a reflection matrix, with the following block-decomposition

$$R = \begin{pmatrix} A & B \\ B^\dagger & D \end{pmatrix},$$

where the blocks $A = A^\dagger$, $D = D^\dagger$ are square matrices, but $B, B^\dagger$ may be rectangular. Let Π be the orthogonal projector (that is actually a diagonal matrix with $0, 1$ diagonal entries) such that

$$A = \Pi R \Pi, \quad B = \Pi R(I - \Pi), \quad B^\dagger = (I - \Pi)R\Pi, \quad D = (I - \Pi)R(I - \Pi).$$

Let us define $Z_\Pi(\phi) := e^{i\phi}\Pi + e^{-i\phi}(I - \Pi)$, and for $\Phi = (\phi_0, \phi_1, \phi_2, \ldots, \phi_d)$ let

$$R_\Phi := Z_\Pi(\phi_d) \cdots R \cdot Z_\Pi(\phi_3) \cdot R \cdot Z_\Pi(\phi_2) \cdot R \cdot Z_\Pi(\phi_1) \cdot R \cdot Z_\Pi(\phi_0).$$

Theorem 1. *Let $\Phi = (\phi_0, \phi_1, \phi_2, \ldots, \phi_d)$, then*

$$R_\Phi = \begin{pmatrix} P_\Phi(A) & B \cdot Q^*_\Phi(D) \\ B^\dagger \cdot Q_\Phi(A) & P^*_\Phi(D) \end{pmatrix}, \tag{1}$$

where the polynomials $P_\Phi, Q_\Phi \in \mathbb{C}[x]$ are determined by by the recurrence relations

$$d = 0: \qquad P_{(\phi_0)} = e^{i\phi_0}, Q_{(\phi_0)} = 0,$$

$$d \to d+1: \qquad \begin{cases} P_{(\phi_0,\phi_1,\ldots,\phi_d,\phi_{d+1})} = e^{i\phi_{d+1}}(xP_{(\phi_0,\phi_1,\ldots,\phi_d)}(x) + (1-x^2)Q_{(\phi_0,\phi_1,\ldots,\phi_d)}(x)), \\ Q_{(\phi_0,\phi_1,\ldots,\phi_d,\phi_{d+1})} = e^{-i\phi_{d+1}}(P_{(\phi_0,\phi_1,\ldots,\phi_d)}(x) - xQ_{(\phi_0,\phi_1,\ldots,\phi_d)}(x)). \end{cases}$$

In particular the polynomials $P_\Phi, Q_\Phi \in \mathbb{C}[x]$ are such that

1.) $\deg(P_\Phi) \le d$ *and** $\deg(Q_\Phi) \le d - 1$,

2.) P_Φ *has parity*† d *and* Q_Φ *has parity* $d - 1$,

3.) $|P_\Phi(x)|^2 + (1 - x^2)|Q_\Phi(x)|^2 = 1$ *for all* $x \in [-1, 1]$.

Moreover, if a pair of polynomials $P, Q \in \mathbb{C}[x]$ satisfies properties 1-2-3 and $\deg(P) = d$, then there exists a sequence of "phases" $\Phi = (\phi_0, \phi_1, \phi_2, \ldots, \phi_d)$ such that $P = P_\Phi$ and $Q = Q_\Phi$.

Note: a slight generalization gives the QSVT version which can be proven the same way, see `https://gilyen.hu/teaching/AdditionalMaterial.pdf`.

6.) Matrix-element-wise reweighing in the energy basis via weighted Heisenberg evolution:
Suppose that for all $\nu \in \mathbb{R}$ we have $f(\nu) = \int_{-\infty}^{\infty} \hat{f}(t)\exp(it\nu)dt$. Let $H = \sum_i E_i|\psi_i\rangle\langle\psi_i|$ be an orthonormal eigendecomposition of the Hermitian matrix H, then

$$f(E_i - E_j)\langle\psi_i|A|\psi_j\rangle = \langle\psi_i|\left(\int_{-\infty}^{\infty} \hat{f}(t)\exp(itH)A\exp(-itH)dt\right)|\psi_j\rangle.$$

7.) (**H**) Quadratic Chebyshev truncation of monomials:
Let $Y_i \in \{-1, 1\}$ be discrete i.i.d. uniform random variables and let $D_s := \sum_{i=1}^{s} Y_i$. Let $T_d(x)$ be the degree-d Chebyshev polynomial of the first kind.

*Our convention is that the 0 polynomial has degree $-\infty$.

†A polynomial is even / odd when all its non-zero coefficients are for even / odd powers. By parity d we mean the parity of the number d, i.e., even if d is even and odd if d is odd.

Theorem 2. *For every $s \geq 0$ integer we have that* $x^s = \mathop{\mathbb{E}}_{Y_1,\ldots,Y_s}[T_{D_s}(x)]$.

Let $\chi(|D_s| \leq d)$ be the indicator for the event $|D_s| \leq d$, then for all $x \in [-1,1]$ we also have that

$$\left| \mathop{\mathbb{E}}_{Y_1,\ldots,Y_s}[T_{D_s}(x)\chi(|D_s| \leq d)] - x^s \right| \leq 2\exp^{-\frac{d^2}{2s}}.$$

8.) (**H**) Periodic discretized wrapping and taking the respective Fourier transforms "commute": Prove the following property connecting discrete and continuous Fourier transformations.

Theorem 3. *Consider the Fourier transform $\hat{f}(\omega) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{e}^{-\mathrm{i}\omega t} f(t)\mathrm{d}t$ of a function $f \in \mathcal{L}_1(\mathbb{R})$. Suppose that a "wrapped around" version of f can be defined such that $p(t) = \sum_{n=-\infty}^{\infty} f(t + nNt_0)$ for almost every $t \in \mathbb{R}$ (i.e., the set of points where the equality does not hold has Lebesgue measure 0), $p(t)$ is continuous at every $\bar{t} \in \mathbb{Z}t_0$ and Riemann integrable on the interval $[-\frac{N}{2}t_0, \frac{N}{2}t_0]$. Let $\omega_0 := \frac{2\pi}{Nt_0}$; if the sequence $k \cdot \hat{f}(k\omega_0)\colon k \in \mathbb{Z}$ is bounded in absolute value, then the limit $\hat{p}(\bar{\omega}) := \lim_{B\to\infty} \sum_{\ell=-B}^{B} \hat{f}(\bar{\omega} + \ell N\omega_0)$ exists for every $\bar{\omega} \in \mathbb{Z}\omega_0$ and $\hat{p}(\bar{\omega})$ is the discrete Fourier transform of $p(\bar{t})$, i.e.,*

$$\hat{p}(\bar{\omega}) = \frac{t_0}{\sqrt{2\pi}} \sum_{\bar{t}\in[N]\cdot t_0} \mathrm{e}^{-\mathrm{i}\bar{\omega}\bar{t}} p(\bar{t}). \tag{2}$$

Hints

Exercise 1: Compute $(\langle 0|\langle 0| \otimes I) \cdot (P^\dagger \otimes I)U(P \otimes I) \cdot (|0\rangle|0\rangle \otimes I)$

Exercise 2: Consider $(I_1 \otimes U_A)(\mathrm{NTOFF}_a \otimes I_m)(X \otimes U_B)$ where the identities I_k act on k qubits and the a-qubit nil-controlled Toffoli is $\mathrm{NTOFF}_a = I_{a+1} + (X - I_1) \otimes |0^a\rangle\langle 0^a|$.

Exercise 3: Compute $(\langle 0|\langle i|U^\dagger) \cdot SWAP \cdot U|0\rangle|j\rangle$

Exercise 4.c: For the spectral decomposition $A^\dagger A = \sum_{i=1}^n \lambda_i |\psi_i\rangle\langle\psi_i|$ study overlaps between the vectors $A|\psi_i\rangle$.

Exercise 5: Use induction and the observation that

$$I = R^\dagger R = RR = \begin{pmatrix} A & B \\ B^\dagger & D \end{pmatrix} \cdot \begin{pmatrix} A & B \\ B^\dagger & D \end{pmatrix} = \begin{pmatrix} A^2 + BB^\dagger & AB + BD \\ B^\dagger A + DB^\dagger & B^\dagger B + D^2 \end{pmatrix}.$$

A full proof can be found in `https://gilyen.hu/teaching/AdditionalMaterial.pdf`.

Exercise 7: The Chebyshev polynomials of the first kind are defined for all $d \in \mathbb{Z}$ via $T_d(\cos\theta) = \cos(d \cdot \theta)$. Use inductively their recursion relation

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x = T_{-1}(x) \end{aligned}$$

$$\forall d \in \mathbb{Z} \colon x \cdot T_d(x) = \frac{T_{d-1}(x) + T_{d+1}(x)}{2}.$$

For the error bound use Chernoff bound. A full proof can be found in [SV14, Theorem 3.1-3.3].

Exercise 8: Let $f \colon [0, 2\pi] \to \mathbb{C}$ be a 2π-periodic Riemann-integrable function and let

$$\hat{f}(r) := \frac{1}{2\pi} \int_0^{2\pi} f(t) \exp(-\mathrm{i}rt) dt.$$

A well-known variant of the inversion theorem in the theory of Fourier series states (cf. [Kö88, Theorem 15.3])) that if $\hat{f}(r) = \mathcal{O}(1/r)$ as $r \to \infty$, moreover f is continuous at t, then

$$\lim_{n\to\infty} \sum_{r=-n}^{n} \hat{f}(r) \exp(\mathrm{i}rt) = f(t).$$

For a full proof of Theorem 3 see [CKBG23, Fact A.1].

References

[CKBG23] Chi-Fang Chen, Michael J. Kastoryano, Fernando G. S. L. Brandão, and András Gilyén. Quantum thermal state preparation. arXiv: 2303.18224, 2023.

[Kö88] Thomas William Körner. *Fourier Analysis*. Cambridge University Press, Cambridge, 1988.

[SV14] Sushant Sachdeva and Nisheeth K. Vishnoi. Faster algorithms via approximation theory. *Found. Trends Theor. Comput. Sci.*, 9(2):125–210, 2014.

Some Solutions

Exercise 2:

$$
\begin{aligned}
(\langle 0^{a+1}| \otimes I_m)(I_1 \otimes U_A)(\mathrm{NTOFF}_a \otimes I_m)(X \otimes U_B)(|0^{a+1}\rangle \otimes I_m)& \\
=&(\langle 0^{a+1}| \otimes I_m)(I_1 \otimes U_A)(X \otimes U_B)(|0^{a+1}\rangle \otimes I_m) && (=0)\\
&+ (\langle 0^{a+1}| \otimes I_m)(I_1 \otimes U_A)(X \otimes |0^a\rangle\langle 0^a| \otimes I_m)(X \otimes U_B)(|0^{a+1}\rangle \otimes I_m)\\
&- (\langle 0^{a+1}| \otimes I_m)(I_1 \otimes U_A)(I_1 \otimes |0^a\rangle\langle 0^a| \otimes I_m)(X \otimes U_B)(|0^{a+1}\rangle \otimes I_m) && (=0)\\
=&(\langle 0^a| \otimes I_m)U_A(|0^a\rangle\langle 0^a| \otimes I_m)U_B(|0^a\rangle \otimes I_m)\\
=&(\langle 0^a| \otimes I_m)U_A(|0^a\rangle \otimes I_m)(\langle 0^a| \otimes I_m)U_B(|0^a\rangle \otimes I_m)\\
=&AB.
\end{aligned}
$$

In a block-matrix representation the same proof can be described as follows. Let

$$
U_A = \begin{pmatrix} R_{00} & R_{0\perp} \\ R_{\perp 0} & R_{\perp\perp} \end{pmatrix} \quad \text{and} \quad U_B = \begin{pmatrix} C_{00} & C_{0\perp} \\ C_{\perp 0} & C_{\perp\perp} \end{pmatrix},
$$

where $A = R_{00}$ and $B = C_{00}$, then

$$
\begin{aligned}
(I_1 \otimes U_A)(\mathrm{NTOFF}_a \otimes I_m)(X \otimes U_B)& \\
&= \begin{pmatrix} R_{00} & R_{0\perp} & & \\ R_{\perp 0} & R_{\perp\perp} & & \\ & & R_{00} & R_{0\perp} \\ & & R_{\perp 0} & R_{\perp\perp} \end{pmatrix} \begin{pmatrix} & & I & \\ & I & & \\ I & & & \\ & & & I \end{pmatrix} \begin{pmatrix} & & C_{00} & C_{0\perp} \\ & & C_{\perp 0} & C_{\perp\perp} \\ C_{00} & C_{0\perp} & & \\ C_{\perp 0} & C_{\perp\perp} & & \end{pmatrix}\\
&= \begin{pmatrix} R_{00} & R_{0\perp} & & \\ R_{\perp 0} & R_{\perp\perp} & & \\ & & R_{00} & R_{0\perp} \\ & & R_{\perp 0} & R_{\perp\perp} \end{pmatrix} \begin{pmatrix} C_{00} & C_{0\perp} & & \\ & & C_{\perp 0} & C_{\perp\perp} \\ & & C_{00} & C_{0\perp} \\ C_{\perp 0} & C_{\perp\perp} & & \end{pmatrix}\\
&= \begin{pmatrix} AB & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}.
\end{aligned}
$$