A simple elementary derivation of Quantum Singular Value Transformation

András Gilyén

November 17, 2023

1 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 $\Phi = (\phi_0, \phi_1, \phi_2, \dots, \phi_d)$ 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 $\Phi = (\phi_0, \phi_1, \phi_2, \dots, \phi_d)$, 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

$$\begin{aligned} d = 0: &\quad P_{(\phi_0)} = e^{i\phi_0}, Q_{(\phi_0)} = 0, \\ d \to d+1: &\quad \begin{cases} P_{(\phi_0,\phi_1,\dots,\phi_d,\phi_{d+1})} = e^{i\phi_{d+1}}(xP_{(\phi_0,\phi_1,\dots,\phi_d)}(x) + (1-x^2)Q_{(\phi_0,\phi_1,\dots,\phi_d)}(x)), \\ Q_{(\phi_0,\phi_1,\dots,\phi_d,\phi_{d+1})} = e^{-i\phi_{d+1}}(P_{(\phi_0,\phi_1,\dots,\phi_d)}(x) - xQ_{(\phi_0,\phi_1,\dots,\phi_d)}(x)). \end{cases} \end{aligned}$$

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* $x \in [-1,1]$.

Proof. First we prove the base case of the recurrence relations. For $d = 0$ we have

$$R_\Phi = Z_\Pi(\phi_0) = \begin{pmatrix} e^{i\phi_0}I & 0 \\ 0 & e^{-i\phi_0}I \end{pmatrix},$$

and thus $P_{(\phi_0)} = e^{i\phi_0}$ and $Q_{(\phi_0)} = 0$.

For proving the recurrence relation the key observation is that $R = R^\dagger = R^{-1}$ and thus we have

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

[*] Take dagger to get the other form ...

[†] 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.

[§] Note that this can be thought of as a complex Pell equation.

Let $\Phi = (\phi_0, \phi_1, \ldots, \phi_d)$, $P'(x) = xP_\Phi(x) + (1-x^2)Q_\Phi(x)$ and $Q'(x) = P_\Phi(x) - xQ_\Phi(x)$ then

$$\begin{aligned}
Z_\Pi(-\phi_{d+1}) \cdot R(\phi_0, \phi_1, \ldots, \phi_d, \phi_{d+1}) &= R \cdot R_\Phi \\
&= \begin{pmatrix} A & B \\ B^\dagger & D \end{pmatrix} \cdot \begin{pmatrix} P_\Phi(A) & B \cdot Q^*_\Phi(D) \\ B^\dagger \cdot Q_\Phi(A) & P^*_\Phi(D) \end{pmatrix} \\
&= \begin{pmatrix} AP_\Phi(A) + BB^\dagger \cdot Q_\Phi(A) & AB \cdot Q^*_\Phi(D) + BP^*_\Phi(D) \\ B^\dagger P_\Phi(A) + DB^\dagger \cdot Q_\Phi(A) & B^\dagger B \cdot Q^*_\Phi(D) + DP^*_\Phi(D) \end{pmatrix} \\
&\overset{(2)}{=} \begin{pmatrix} AP_\Phi(A) + (I - A^2) \cdot Q_\Phi(A) & -BD \cdot Q^*_\Phi(D) + BP^*_\Phi(D) \\ B^\dagger P_\Phi(A) - B^\dagger A \cdot Q_\Phi(A) & (I - D^2) \cdot Q^*_\Phi(D) + DP^*_\Phi(D) \end{pmatrix} \\
&= \begin{pmatrix} P'(A) & B \cdot Q'^*(D) \\ B^\dagger \cdot Q'_\Phi(A) & P'^*(D) \end{pmatrix}.
\end{aligned}$$

Multiplying both equations with $Z_\Pi(\phi_{d+1})$ form the left we recover the claimed recurrence relation:

$$R(\phi_0, \phi_1, \phi_2, \ldots, \phi_d, \phi_{d+1}) = \begin{pmatrix} e^{i\phi_{d+1}} P'(A) & B \cdot e^{i\phi_{d+1}} Q'^*(D) \\ B^\dagger \cdot e^{-i\phi_{d+1}} Q'_\Phi(A) & e^{-i\phi_{d+1}} P'^*(D) \end{pmatrix}.$$

The properties 1-2 directly follow from the recurrence relations, and 3 follows from the fact that R_Φ is always unitary, in particular choosing $R = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}$ its first column has norm 1. □

Note that Szegedy walks are a special case corresponding to $\Phi_d := \left(0, \overbrace{\frac{\pi}{2}, \frac{\pi}{2}, \ldots, \frac{\pi}{2}}^{d\times}\right)$, so that $Z_\Pi \equiv i(2\Pi - I)$ apart from the first operator which is identity. Then $P_{\Phi_d} = i^d T_d(x)$ and $Q_{\Phi_d} = -i^d U_{d-1}(x)$, where T_d and U_d are Chebyshev polynomials of the first and second kind respectively, as shown by the following joint recurrence relations of Chebyshev polynomials:

$$\begin{aligned}
T_{d+1}(x) &= x \cdot T_d(x) - (1-x^2)\, U_{d-1}(x), \\
U_d(x) &= x \cdot U_{d-1}(x) + T_d(x).
\end{aligned}$$

Corollary 2 (Explicit form of Szegedy walk iterations)**.**

$$((2\Pi - I)R)^d = \begin{pmatrix} T_d(A) & B \cdot (-1)^{d-1} U_{d-1}(D) \\ -B^\dagger \cdot U_{d-1}(A) & (-1)^d T_d(D) \end{pmatrix} = \begin{pmatrix} T_d(A) & U_{d-1}(A) \cdot B \\ -B^\dagger \cdot U_{d-1}(A) & (-1)^d T_d(D) \end{pmatrix}.$$

Proof. The first equality follows from Theorem 1 using the above observation $P_{\Phi_d} = i^d T_d(x)$, $Q_{\Phi_d} = -i^d U_{d-1}(x)$ after dividing everything with the global phase i^d. The second equality follows from the observation that $R((2\Pi - I)R)^{d-1}$ is Hermitian. □

Lemma 3. *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 $Q = Q_\Phi$.*

Proof. This can be proven using the recurrence relations. For the base case $d = 0$ this follows immediately and the rest can be proven by induction.

For the induction step observe that for $x \in [-1, 1]$ we have $|P(x)|^2 = P(x)P^*(x)$ and $|Q(x)|^2 = Q(x)Q^*(x)$, and therefore 3 implies the polynomial identity $P(x)P^*(x) + (1-x^2)Q(x)Q^*(x) = 1$. Since $d \geq 1$ the leading coefficient p_d of P must have the same magnitude as the leading coefficient q_{d-1} of Q. Let $\phi \in \mathbb{R}$ be such that $e^{i2\phi} = p_d/q_{d-1}$ and let $\tilde{P} := xe^{-i\phi}P + (1-x^2)e^{i\phi}Q$ and $\tilde{Q} := e^{-i\phi}P - xe^{i\phi}Q$, then the leading coefficients cancel and so $\deg(\tilde{P}) \leq d-1$ and $\deg(\tilde{Q}) \leq d-2$. By construction $\tilde{P}, \tilde{Q}$ also satisfy 2. Property 3 is also satisfied since

$$\begin{pmatrix} \tilde{P}(x) \\ \sqrt{1-x^2}\tilde{Q}(x) \end{pmatrix} = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \cdot \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \cdot \begin{pmatrix} P(x) \\ \sqrt{1-x^2}Q(x) \end{pmatrix},$$

where the vector on the right has norm 1 by assumption and it is multiplied by two unitary, i.e., norm preserving matrix. Inverting this equation we get that

$$\begin{pmatrix} P(x) \\ \sqrt{1-x^2}Q(x) \end{pmatrix} = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix} \cdot \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \cdot \begin{pmatrix} \tilde{P}(x) \\ \sqrt{1-x^2}\tilde{Q}(x) \end{pmatrix}.$$

By the induction hypothesis $\tilde{P} = P_\Phi$ and $\tilde{Q} = Q_\Phi$ for some $\Phi = (\phi_0, \phi_1, \ldots, \phi_k)$ and $k \leq d-1$. By the above equation and the recurrence relation we get that $P = P_{(\phi_0,\phi_1,\ldots,\phi_k,\phi)}$ and $Q = Q_{(\phi_0,\phi_1,\ldots,\phi_k,\phi)}$. Since $\deg(P) = d$ we must have that $k \geq d-1$ and thus $k = d-1$. □

2 Quantum Singular Value Transformation (QSVT)

Let $U \in \mathbb{C}^{N\times N}$ be a unitary matrix with the following block-like decomposition

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where the submatrices may be rectangular and can have different (but matching) sizes. Let Π, Π' be the orthogonal projectors such that

$$A = \Pi' U \Pi|_{\mathrm{im}(\Pi)\to\mathrm{im}(\Pi')}, \qquad B = \Pi' U (I-\Pi)|_{\mathrm{im}(I-\Pi)\to\mathrm{im}(\Pi')},$$
$$C = (I-\Pi') U \Pi|_{\mathrm{im}(\Pi)\to\mathrm{im}(I-\Pi')}, \qquad D = (I-\Pi') U (I-\Pi)|_{\mathrm{im}(I-\Pi)\to\mathrm{im}(I-\Pi')}.$$

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[¶]

$$U_\Phi := Z_{\Pi^{(\prime)}}(\phi_d) \cdots U^\dagger \cdot Z_{\Pi'}(\phi_3) \cdot U \cdot Z_\Pi(\phi_2) \cdot U^\dagger \cdot Z_{\Pi'}(\phi_1) \cdot U \cdot Z_\Pi(\phi_0).$$

For a polynomial P and a matrix M with singular value decomposition $M = \sum_i \sigma_i |\phi_i\rangle\langle\psi_i|$ let us denote by $[P(x)|x = M^{(SV)}]$ the matrix we get by applying P to M's singular values as follows[‖]

$$[P(x)|x = M^{(SV)}] := \begin{cases} \sum_i P(\sigma_i)|\phi_i\rangle\langle\psi_i| & \text{for odd } P, \\ \sum_i P(\sigma_i)|\psi_i\rangle\langle\psi_i| & \text{for even } P. \end{cases}$$

Theorem 4. *We have that*

$$U_\Phi = \begin{cases} \begin{pmatrix} AP(A^\dagger A) & BQ^*(D^\dagger D) \\ CQ(A^\dagger A) & DP^*(D^\dagger D) \end{pmatrix}, & \text{for } d \text{ odd} \\ \begin{pmatrix} P(A^\dagger A) & C^\dagger D Q^*(D^\dagger D) \\ B^\dagger A Q(A^\dagger A) & P^*(D^\dagger D) \end{pmatrix}, & \text{for } d \text{ even,} \end{cases} \tag{3}$$

where $P, Q \in \mathbb{C}[x]$ are some polynomials s.t. $\deg(P) \leq \frac{d}{2}$, $\deg(Q) \leq \frac{d-1}{2}$. *Alternatively, we can write*

$$U_\Phi = \begin{cases} \begin{pmatrix} [P_\Phi(x)|x = A^{(SV)}] & B \cdot [Q^*_\Phi(x)|x = D^{(SV)}] \\ C \cdot [Q_\Phi(x)|x = A^{(SV)}] & [P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} & \text{for } d \text{ odd} \\ \begin{pmatrix} [P_\Phi(x)|x = A^{(SV)}] & C^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & [P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} & \text{for } d \text{ even,} \end{cases} \tag{4}$$

where the polynomials $P_\Phi, Q_\Phi \in \mathbb{C}[x]$ are determined by by the recurrence relations in Theorem 1.

[¶]The leading matrix term in the product is $Z_\Pi(\phi_d)$ if d is even and $Z_{\Pi'}(\phi_d)$ if d is odd.

[‖]For this to be well-defined in the even case we require that $|\psi_i\rangle$ span the domain of M, which in our case is either $\mathrm{im}(\Pi)$ or $\mathrm{im}(I-\Pi)$. In case M is rectangular with more columns than rows this can be formally achieved by adding dummy terms to the singular value decomposition: $0 \cdot |\varnothing\rangle\langle\psi_i|$, where $|\varnothing\rangle$ is the 0 vector so that $|\psi_i\rangle$ form an orthonormal basis. This is needed to properly handle the constant term of the polynomial: $[1|x = M^{(SV)}] = \Pi_{\mathrm{dom}(M)}$.

Proof. First we reduce Eq. (3) to Eq. (4) by observing that $P(M^\dagger M) = [P(x^2)|x = M^{(SV)}]$ and $MP(M^\dagger M) = [xP(x^2)|x = M^{(SV)}]$ for any matix M, which directly follows from the definition.

Now we prove the base case of the recurrence relations. For $d = 0$ we have

$$U_\Phi = Z_\Pi(\phi_0) = \begin{pmatrix} e^{i\phi_0} I & 0 \\ 0 & e^{-i\phi_0} I \end{pmatrix},$$

and thus $P_{(\phi_0)} = e^{i\phi_0}$ and $Q_{(\phi_0)} = 0$.

For proving the recurrence relation the key observation is that due to unitarity we have that

$$I = UU^\dagger = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \begin{pmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{pmatrix} = \begin{pmatrix} AA^\dagger + BB^\dagger & AC^\dagger + BD^\dagger \\ CA^\dagger + DB^\dagger & CC^\dagger + DD^\dagger \end{pmatrix}, \tag{5}$$

and

$$I = U^\dagger U = \begin{pmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A^\dagger A + C^\dagger C & A^\dagger B + C^\dagger D \\ B^\dagger A + D^\dagger C & B^\dagger B + D^\dagger D \end{pmatrix}. \tag{6}$$

Let $\Phi = (\phi_0, \phi_1, \phi_2, \ldots, \phi_d)$. First we prove the case when d is even using Equation (5):

$$\begin{aligned}
&Z_{\Pi'}(-\phi_{d+1}) \cdot U(\phi_0, \phi_1, \phi_2, \ldots, \phi_d, \phi_{d+1}) \\
&= U \cdot U_\Phi \\
&= \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \begin{pmatrix} [P_\Phi(x)|x = A^{(SV)}] & C^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & [P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&= \begin{pmatrix} A[P_\Phi(x)|x = A^{(SV)}] + BB^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & AC^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + B[P^*_\Phi(x)|x = D^{(SV)}] \\ C[P_\Phi(x)|x = A^{(SV)}] + DB^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & CC^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + D[P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&\overset{(5)}{=} \begin{pmatrix} A[P_\Phi(x)|x = A^{(SV)}] + (I - AA^\dagger) \cdot [Q_\Phi(x)|x = A^{(SV)}] & -BD^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + B[P^*_\Phi(x)|x = D^{(SV)}] \\ C[P_\Phi(x)|x = A^{(SV)}] - CA^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & (I - DD^\dagger) \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + D[P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&= \begin{pmatrix} [xP_\Phi(x) + (1 - x^2)Q_\Phi(x)|x = A^{(SV)}] & B[P^*_\Phi(x) - xQ^*_\Phi(x)|x = D^{(SV)}] \\ C[P_\Phi(x) - xQ_\Phi(x)|x = A^{(SV)}] & [xP^*_\Phi(x) + (1 - x^2)Q^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix}.
\end{aligned}$$

Multiplying both equations with $Z_{\Pi'}(\phi_{d+1})$ form the left we recover the claimed recurrence relation.

The case when d is odd can proven analogously using Equation (6):

$$\begin{aligned}
&Z_{\Pi}(-\phi_{d+1}) \cdot U(\phi_0, \phi_1, \phi_2, \ldots, \phi_d, \phi_{d+1}) \\
&= U^\dagger \cdot U_\Phi \\
&= \begin{pmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{pmatrix} \cdot \begin{pmatrix} [P_\Phi(x)|x = A^{(SV)}] & B \cdot [Q^*_\Phi(x)|x = D^{(SV)}] \\ C \cdot [Q_\Phi(x)|x = A^{(SV)}] & [P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&= \begin{pmatrix} A^\dagger[P_\Phi(x)|x = A^{(SV)}] + C^\dagger C \cdot [Q_\Phi(x)|x = A^{(SV)}] & A^\dagger B \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + C^\dagger[P^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger[P_\Phi(x)|x = A^{(SV)}] + D^\dagger C \cdot [Q_\Phi(x)|x = A^{(SV)}] & B^\dagger B \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + D^\dagger[P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&\overset{(6)}{=} \begin{pmatrix} A^\dagger[P_\Phi(x)|x = A^{(SV)}] + (I - A^\dagger A) \cdot [Q_\Phi(x)|x = A^{(SV)}] & -C^\dagger D \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + C^\dagger[P^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger[P_\Phi(x)|x = A^{(SV)}] - B^\dagger A \cdot [Q_\Phi(x)|x = A^{(SV)}] & (I - D^\dagger D) \cdot [Q^*_\Phi(x)|x = D^{(SV)}] + D^\dagger[P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \\
&= \begin{pmatrix} [xP_\Phi(x) + (1 - x^2)Q_\Phi(x)|x = A^{(SV)}] & C^\dagger[P^*_\Phi(x) - xQ^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger[P_\Phi(x) - xQ_\Phi(x)|x = A^{(SV)}] & [xP^*_\Phi(x) + (1 - x^2)Q^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix}.
\end{aligned}$$

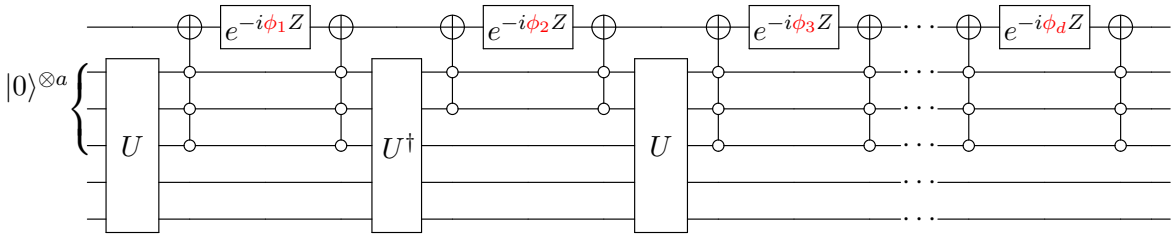
Multiplying both equations with $Z_{\Pi}(\phi_{d+1})$ form the left we recover the claimed recurrence relation. □

A useful observation is that $P_{-\Phi} = P^*_\Phi$ and $Q_{-\Phi} = Q^*_\Phi$ as follows from the recurrence relations. It is proven in [Gil19, Theorem 2.2.3.] that for a degree-d even/odd $P \in \mathbb{R}[x]$ there exists a Φ of length $d + 1$ such that $P = \Re(P_\Phi)$ if and only if $|P(x)| \leq 1$ for all $x \in [-1, 1]$. If $d > 0$, then without loss of generality we can also assume that $\phi_0 = 0$, since we only care about P_Φ and so we might simultaneously modify $\phi_d \leftarrow \phi_d + \phi_0$ and $\phi_0 \leftarrow 0$ without affecting P_Φ. Since $\Re(P_\Phi) = \frac{P_\Phi + P^*_\Phi}{2} = \frac{P_\Phi + P_{-\Phi}}{2}$, using linear combination of unitaries we get the following corollary.

Theorem 5 (Quantum Singular Value Transformation (QSVT)[GSLW19]). *Let $P\colon [-1,1] \mapsto [-1,1]$ be a degree-d even or odd polynomial. Suppose that U is a block-encoding of $A = (\langle 0^a| \otimes I)U(|0^b\rangle \otimes I)$. Then $V := (H \otimes I)\tilde{U}_\Phi(H \otimes I)$ is a block-encoding of*

$$[P(x)|x = A^{(SV)}] = (\langle 0^{a+1}| \otimes I)V(|0^{b+1}\rangle \otimes I), \tag{7}$$

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



Proof. Here $\Pi = |0^a\rangle\langle 0^a|$ and $\Pi' = |0^b\rangle\langle 0^b|$. The key observation is that in the above circuit implementation if the first qubit is in state $|0\rangle$, then the generalized-Toffoli sandwiched Z rotation gates implement $Z_{\Pi^{(\prime)}}(\phi_j)$, while if the first qubit is in state $|1\rangle$ they implement $Z_{\Pi^{(\prime)}}(-\phi_j)$. Therefore $\tilde{U}_\Phi = |0\rangle\langle 0| \otimes U_\Phi + |1\rangle\langle 1| \otimes U_{-\Phi}$ and so $(\langle +| \otimes I)\tilde{U}_\Phi(|+\rangle \otimes I) = \frac{U_\Phi + U_{-\Phi}}{2}$. □

3 Applications of QSVT

Hamiltonian simulation: $e^{itH} = \cos(tH) + i\sin(tH)$. Find even / odd polynomial approximations of $\cos(tx)$ and $\sin(tx)$ as in Exercise 3 and apply linear combination of unitaries to approximately block-encode $e^{itH}/2$. Finally, apply the degree 3 Chebyshev to the singular values of $e^{itH}/2$ motivated by the fact that $T_3(e^{itH}/2) = e^{itH}$. Also see [dW19, Chapter 9.4].

Quantum linear equation solving (HHL). See [dW19, Chapter 10.1] and the exercises below.

Exercises

1.) Show that the operator norm of A is $\|A\| = \sigma_1$.

2.) Let $f\colon \mathbb{R} \to \mathbb{C}$, and $P \in \mathbb{C}[x]$ a polynomial such that $|f(x) - P(x)| \leq \varepsilon$ for all $x \in S \subseteq \mathbb{R}$. Suppose that the singular values of A are elements of the set $\sigma_i \in S$ for all $i \in \{1, 2, \ldots, d\}$. Show that $B := \sum_{i=1}^d f(\sigma_i)|w_i\rangle\langle v_i|$ and $\widetilde{B} := \sum_{i=1}^d P(\sigma_i)|w_i\rangle\langle v_i|$ are ε-close, i.e., $\left\|B - \widetilde{B}\right\| \leq \varepsilon$.

3.) The Taylor series of the exponential function gives us $e^{itx} = \sum_{k=0}^\infty \frac{(itx)^k}{k!}$. Let $P(x) := \sum_{k=0}^K \frac{(itx)^k}{k!}$ for $K = \lceil 2et + \log_2(1/\varepsilon)\rceil$, where $\varepsilon \in (0, \frac{1}{2}]$. Prove that $|e^{itx} - P(x)| \leq \varepsilon$ for every $x \in [-1, 1]$. (**H**)

4.) This exercise shows how to solve a linear equation of the form $Ax = b$, when the equation might be under/over-determined. The least square solution is given by A^+b, where A^+ is the Moore-Penrose pseudoinverse of A defined as $A^+ := \sum_{i=1}^d \frac{1}{\sigma_i}|v_i\rangle\langle w_i|$.

(a) Prove that $(AA^+)A = A$ and $A^+(AA^+) = A^+$. This shows that A^+ indeed acts as we expect from a generalized inverse.

(b) Suppose that U is a block-encoding of A, s.t., $A = (\langle 0| \otimes I)U(|0\rangle \otimes I)$, and $\|A^+\| \leq \kappa$. Describe a bounded set S that contains the singular values of any such matrix A, but is disjoint from some interval of the form $(0, a)$ for some $a > 0$. What is the largest a that we can choose?

[**]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 $a = 3$, $b = 2$.

(c) Construct an approximate block-encoding V of $A^+/(2\kappa)$ such that

$$\left\| A^+/(2\kappa) - (\langle 00| \otimes I)V(|00\rangle \otimes I) \right\| \leq \varepsilon,$$

and V uses $\mathcal{O}(\kappa \log(1/\varepsilon))$-times the block-encoding U and its inverse $U^\dagger$. (**H**)

(d) Assume for simplicity that $A^+/(2\kappa) = (\langle 00| \otimes I)V(|00\rangle \otimes I)$ holds exactly. Suppose that W is a quantum circuit that maps $|0^n\rangle \to |b\rangle$. Give a quantum algorithm that prepares a quantum state proportional to $A^+|b\rangle$ with high probability with $\mathcal{O}(\kappa)$ uses of the quantum circuits V and W. What does it tell us about the complexity of preparing a quantum state proportional to the least-square solution $A^+|b\rangle$ given the block-encoding of A?

Hints

Exercise 3: You can use the following crude version of Stirling's approximation: $(\frac{n}{e})^n \leq n!$ for all $n \in \mathbb{N}$.

Exercise 4c: You can use the following polynomial approximation result [Gil19, Corollary 3.4.13.] without proof: for every $\kappa > 1$ and $\varepsilon < 1$ there is an odd polynomial $P \in \mathbb{R}[x]$ of degree $\mathcal{O}(\kappa \log(1/\varepsilon))$, such that $|P(x)| \leq 1$ for all $x \in [-1, 1]$, and $|P(x) - 1/(2\kappa x)| \leq \varepsilon$ for all $x \in [1/\kappa, 1]$.

References

[Gil19] András Gilyén. *Quantum Singular Value Transformation & Its Algorithmic Applications*. PhD thesis, University of Amsterdam, 2019.

[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)*, pages 193–204, 2019. arXiv: `1806.01838`

[dW19] Ronald de Wolf. Quantum computing: Lecture notes, 2019. arXiv: `1907.09415v5`