2 Proving QSVT

Let's start by recalling some statements from the previous lecture.

Definition 1.1 (Variant of [GSLW19, Definition 43], [Ral20, Definition 1])**.** Given $A \in \mathbb{C}^{r\times c}$, we say $U \in \mathbb{C}^{d\times d}$ is a Q-block encoding of A if U is implementable with $\mathcal{O}(Q)$ gates and

$$B_{\mathrm{L},1}^\dagger U B_{\mathrm{R},1} = A, \tag{1}$$

where $B_{\mathrm{L},1} \in \mathbb{C}^{d\times r}, B_{\mathrm{R},1} \in \mathbb{C}^{d\times c}$ are the first r and c columns of the identity matrix. Equivalently,

$$U = \begin{pmatrix} A & \cdot \\ \cdot & \cdot \end{pmatrix}, \tag{2}$$

where $\cdot$ denotes arbitrary elements of U. We denote $\Pi_{\mathrm{L}} = B_{\mathrm{L},1}B_{\mathrm{L},1}^\dagger$, $\Pi_{\mathrm{R}} = B_{\mathrm{R},1}B_{\mathrm{R},1}^\dagger$ to be the corresponding projections onto the spans of $B_{\mathrm{L},1}$ and $B_{\mathrm{R},1}$, respectively.

And the statement we wanted to prove in this lecture.

Theorem 1.10 ([GSLW19, Theorem 17 and Corollary 18])**.** *If a polynomial with real coefficients $p \in \mathbb{R}[x]$ is even or odd and satisfies $|p(x)| \le 1$ for all $x \in [-1,1]$, then we can convert a Q-block encoding of A to a $d(\log(d)+Q)$-block encoding of $p^{(\mathrm{SV})}(A)$.*

We begin with the case where A is a scalar and $U \in \mathbb{C}^{2\times 2}$; this is known as quantum signal processing. Then, we show that the circuit used for the scalar case "lifts" to the matrix case; to do this, we use an argument with block matrices.

2.1 Quantum signal processing (QSP)

Definition 2.1 (Quantum signal processing)**.** For a sequence of phase factors $\Phi = \{\phi_j\} \in \mathbb{R}^{n+1}$, it defines a *quantum signal processing* circuit[1]

$$\mathbf{QSP}(\Phi, x) \coloneqq \left(\prod_{j=1}^{n} \underbrace{\begin{pmatrix} e^{\mathrm{i}\phi_j} & 0 \\ 0 & e^{-\mathrm{i}\phi_j} \end{pmatrix}}_{e^{\mathrm{i}\phi_j\sigma_z}} \underbrace{\begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}}_{=:R(x)} \right) \begin{pmatrix} e^{\mathrm{i}\phi_0} & 0 \\ 0 & e^{-\mathrm{i}\phi_0} \end{pmatrix}. \tag{3}$$

Here, the product goes from n on the left-hand side to 1 on the right-hand side.

The idea of QSP is that we can perform a *known* function on an *unknown* (parametrized) operator with these interleaved rotations.

Definition 2.2 ([GSLW19, Corollary 8])**.** We say that a polynomial $p(x) \in \mathbb{C}[x]$ is *QSP-achievable* if there is a sequence of phase factors $\Phi = \{\phi_j\} \in \mathbb{R}^{n+1}$ such that

$$\mathbf{QSP}(\Phi, x) = \begin{pmatrix} p(x) & \cdot \\ \cdot & \cdot \end{pmatrix}. \tag{4}$$

To find out what polynomials are QSP-achievable, we first take a look at what the form of QSP is. It turns out that we can express it as a recurrence of polynomials.

[1] We define QSP with the reflection operation $R(x)$; a different convention is to use the rotation $e^{\mathrm{i}\arccos(x)\sigma_x} = \left(\begin{smallmatrix} x & \mathrm{i}\sqrt{1-x^2} \\ \mathrm{i}\sqrt{1-x^2} & x \end{smallmatrix}\right)$, denoted $W(x)$ in [GSLW19]. These two types of circuits are equivalent up to a shift in phase factors [MRTC21, Appendix A.2]. Using $W(x)$ is perhaps more natural, since then this corresponds to alternating rotations in the σ_X and σ_Z basis.

Lemma 2.3 (QSP as a recurrence)**.** *For some phase factors $\Phi = \{\phi_j\} \in \mathbb{R}^{n+1}$,*

$$\mathbf{QSP}(\{\phi_j\}_{0\le j\le k}, x) = \begin{pmatrix} p_k(x) & \overline{q_k}(-x)\sqrt{1-x^2} \\ q_k(x)\sqrt{1-x^2} & \overline{p_k}(-x) \end{pmatrix}, \tag{5}$$

where $p_k(x)$ and $q_k(x)$ satisfy the following recurrence relation:

$$p_{k+1}(x) = e^{\mathrm{i}\phi_{k+1}}(xp_k(x) + (1-x^2)q_k(x)); \tag{6}$$
$$q_{k+1}(x) = e^{-\mathrm{i}\phi_{k+1}}(p_k(x) - xq_k(x)). \tag{7}$$

For the base case, $p_0(x) = e^{\mathrm{i}\phi_0}$ and $q_0(x) = 0$.

Proof. The base case is because

$$\mathbf{QSP}(\{\phi_0\}, x) = \begin{pmatrix} e^{\mathrm{i}\phi_0} & \\ & e^{-\mathrm{i}\phi_0} \end{pmatrix} \tag{8}$$

For the inductive case, we just do the annoying computation.

$$\mathbf{QSP}(\{\phi_j\}_{0\le j\le k+1}, x) \tag{9}$$
$$= e^{\mathrm{i}\phi_{k+1}\sigma_z} R(x) \cdot \mathbf{QSP}(\{\phi_j\}_{0\le j\le k}, x) \tag{10}$$
$$= \begin{pmatrix} e^{\mathrm{i}\phi_{k+1}}x & e^{\mathrm{i}\phi_{k+1}}\sqrt{1-x^2} \\ e^{-\mathrm{i}\phi_{k+1}}\sqrt{1-x^2} & -e^{-\mathrm{i}\phi_{k+1}}x \end{pmatrix} \begin{pmatrix} p_k(x) & \overline{q_k}(-x)\sqrt{1-x^2} \\ q_k(x)\sqrt{1-x^2} & \overline{p_k}(-x) \end{pmatrix} \tag{11}$$
$$= \begin{pmatrix} e^{\mathrm{i}\phi_{k+1}}(xp_k(x) + (1-x^2)q_k(x)) & e^{\mathrm{i}\phi_{k+1}}(\overline{p_k}(-x) + x\overline{q_k}(-x))\sqrt{1-x^2} \\ e^{-\mathrm{i}\phi_{k+1}}(p_k(x) - xq_k(x))\sqrt{1-x^2} & e^{-\mathrm{i}\phi_{k+1}}(-x\overline{p_k}(-x) + (1-x^2)\overline{q_k}(-x)) \end{pmatrix} \tag{12}$$
$$= \begin{pmatrix} p_{k+1}(x) & \overline{q_{k+1}}(-x)\sqrt{1-x^2} \\ q_{k+1}(x)\sqrt{1-x^2} & \overline{p_{k+1}}(-x) \end{pmatrix} \tag{13}$$

Feel free to stare at the last line for a little bit to confirm indeed that the entries all match up to what I claim them to be. □

Theorem 2.4 ([GSLW19, Theorem 3])**.** *A degree-n polynomial $p(x) \in \mathbb{C}[x]$ is QSP-achievable with some $\Phi \in \mathbb{R}^{n+1}$ if and only if there is some polynomial $q(x)$ such that:*

(a) q has degree $\le n-1$;

(b) (p, q) are (even, odd) or (odd, even);

(c) $|p(x)|^2 + (1-x^2)|q(x)|^2 \equiv 1$.

Proof. First, we consider the "only if" direction. Suppose $p(x)$ is QSP-achievable with the phase factors $\Phi \in \mathbb{R}^{n+1}$. Then, by Lemma 2.3, there is some $q(x)$ such that

$$\mathbf{QSP}(\Phi, x) = \begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix},$$

derived from the recurrence described in that lemma. From this recurrence, we can verify that at all times, conditions (a) and (b) are satisfied. Finally, condition (c) is always satisfied because $\mathbf{QSP}(\Phi, x)$ is a product of unitary matrices, and so is unitary: the first column having norm one is equivalent to $|p(x)|^2 + (1-x^2)|q(x)|^2 = p(x)\overline{p}(x) + (1-$

$x^2)q(x)\overline{q}(x) = 1$, and this argument works for every $x \in [-1, 1]$. Because it holds for infinitely many x, the equality holds as polynomials.

Second, we consider the "if" direction. Suppose we have some $p(x)$ of degree n and $q(x)$ satisfying (a), (b), and (c). We want to construct phase factors that implement $p(x)$. We proceed by induction: when $n = 0$, this means that $p(x)$ is scalar and $q(x)$ has degree ≤ -1 (meaning it must be zero). Thus, $p(x) \equiv e^{i\phi}$ for some ϕ; we can implement this with $\Phi = \{\phi\}$. For the inductive step, consider $p(x)$ of degree $n + 1$. If we could show that there exists some φ such that

$$(e^{i\varphi\sigma_z}R(x))^\dagger \begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix} = \begin{pmatrix} p_\downarrow(x) & \overline{q_\downarrow}(-x)\sqrt{1-x^2} \\ q_\downarrow(x)\sqrt{1-x^2} & \overline{p_\downarrow}(-x) \end{pmatrix} \tag{14}$$

for $p_\downarrow, q_\downarrow$ some even/odd polynomials of one degree lower than p and q, then we would be done. By assumption, the matrices on the left-hand side of Eq. (14) are unitary, so the right-hand side matrix is also unitary. Thus, $p_\downarrow$ and $q_\downarrow$ satisfy all the properties of the induction hypothesis, and there are phase factors $\{\phi_0, \ldots, \phi_n\} \in \mathbb{R}^{n+1}$ giving the equality

$$(e^{i\varphi\sigma_z}R(x))^\dagger \begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix} = \mathbf{QSP}(\{\phi_0, \ldots, \phi_n\}, x). \tag{15}$$

$$\begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix} = \mathbf{QSP}(\{\phi_0, \ldots, \phi_n, \varphi\}, x) \tag{16}$$

So it comes down to finding the right value of φ that could remove a degree from p and q in Eq. (14). By properties (a) and (b), we can write

$$p(x) = a_{n+1}x^{n+1} + a_{n-1}x^{n-1} + \cdots \tag{17}$$

$$q(x) = b_n x^n + a_{n-2}x^{n-2} + \cdots \tag{18}$$

The condition (c) implies that $|a_{n+1}| = |b_n|$. Now, let's do the annoying matrix calculation we were putting off. Since $R(x)$ is its own inverse, $(e^{i\varphi\sigma_z}R(x))^\dagger = R(x)e^{-i\varphi\sigma_z}$, so

$$(e^{i\varphi\sigma_z}R(x))^\dagger \begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix} \tag{19}$$

$$= \begin{pmatrix} e^{-i\varphi}x & e^{i\varphi}\sqrt{1-x^2} \\ e^{-i\varphi}\sqrt{1-x^2} & -e^{i\varphi}x \end{pmatrix} \begin{pmatrix} p(x) & \overline{q}(-x)\sqrt{1-x^2} \\ q(x)\sqrt{1-x^2} & \overline{p}(-x) \end{pmatrix} \tag{20}$$

$$= \begin{pmatrix} e^{-i\varphi}p(x) + e^{i\varphi}(1-x^2)q(x) & (e^{i\varphi}\overline{p}(-x) + e^{-i\varphi}x\overline{q}(-x))\sqrt{1-x^2} \\ (e^{-i\varphi}p(x) - e^{i\varphi}xq(x))\sqrt{1-x^2} & -e^{i\varphi}x\overline{p}(-x) + e^{-i\varphi}(1-x^2)\overline{q}(-x) \end{pmatrix} \tag{21}$$

So, we need the following polynomials to have lower degree:

$$p_\downarrow(x) = e^{-i\varphi}p(x) + e^{i\varphi}(1-x^2)q(x) \tag{22}$$

$$q_\downarrow(x) = e^{-i\varphi}p(x) - e^{i\varphi}xq(x) \tag{23}$$

The "leading" coefficient of x^{n+1} for $p_\downarrow$ and x^n for $q_\downarrow$ are the same: $e^{-i\varphi}a_{n+1} - e^{i\varphi}b_n$. If we choose φ such that $e^{i\varphi} = \sqrt{a_{n+1}/b_n}$, then this coefficient is 0, and so the degrees of $p_\downarrow$ and $q_\downarrow$ are $\leq n-1$ and $\leq n-2$, as desired. □

The characterization of when a polynomial $p(x)$ is QSP-achievable is still quite difficult to understand. With some more work, we can give a clearer understanding of QSP-achievable polynomials, if we give up the imaginary degree of freedom in our polynomials.

Theorem 2.5 ([GSLW19, Theorem 5, Lemma 6])**.** *Let $p_{\mathrm{Re}}(x), q_{\mathrm{Re}}(x) \in \mathbb{R}[x]$ be real-valued polynomials with p of degree n. Then there exist $p, q \in \mathbb{C}[x]$ such that (p, q) is QSP-achievable and $p_{\mathrm{Re}} = \mathrm{Re}(p)$, $q_{\mathrm{Re}} = \mathrm{Re}(q)$ if and only if*

(a) q_{Re} has degree $\leq n - 1$;

(b) $(p_{\mathrm{Re}}, q_{\mathrm{Re}})$ are (even, odd) or (odd, even);

(c') $(p_{\mathrm{Re}}(x))^2 + (1 - x^2)(q_{\mathrm{Re}}(x))^2 \leq 1$ for $x \in [-1, 1]$.

What's happening here is that if we have real polynomials where the "unit norm" constraint is merely an inequality (c'), then we can add imaginary components to make it an equality, so that by Theorem 2.4 these supplemented polynomials are achievable.

Proof. The "only if" direction is the easy one: if we have p, q QSP-achievable, then their real parts satisfy (a), (b), and (c') by Theorem 2.4.

The "if" direction requires some work: given p_{Re} and q_{Re}, we need to find some $p_{\mathrm{Im}} \in \mathbb{R}[x]$ and $q_{\mathrm{Im}} \in \mathbb{R}[x]$ of the right degree and parity such that $p \coloneqq p_{\mathrm{Re}} + \mathrm{i}p_{\mathrm{Im}}$ and $q \coloneqq q_{\mathrm{Re}} + \mathrm{i}q_{\mathrm{Im}}$ satisfy

$$|p(x)|^2 + (1 - x^2)|q(x)|^2 = p_{\mathrm{Re}}^2 + p_{\mathrm{Im}}^2 + (1 - x^2)(q_{\mathrm{Re}}^2 + q_{\mathrm{Im}}^2) \equiv 1.$$

Then we would be done by Theorem 2.4. Consider $1 - p_{\mathrm{Re}}^2 - (1 - x^2)q_{\mathrm{Re}}^2$, which we know is non-negative in $x \in [-1, 1]$ by assumption (c'). *Ewin: I don't think we'll have time to cover this, you can take this non-negative polynomial and prove that it can be written in this $p_{\mathrm{Im}}^2 + (1 - x^2)q_{\mathrm{Im}}^2$ form. Since this form is closed under taking products, it suffices to consider irreducible polynomials (that is, polynomials that can't be further decomposed into roots without making coefficients complex). This is some casework.* □

From this, we can get our desired block-encodings, at least in this scalar case. For some even or odd $p(x) \in \mathbb{R}[x]$, by Theorem 2.5, we can find a phase sequence Φ such that $\mathbf{QSP}(\Phi, x)$ has $p(x) + \mathrm{i}p_{\mathrm{Im}}(x)$ in the top-left corner for some $p_{\mathrm{Im}}(x) \in \mathbb{R}[x]$. Then $\mathbf{QSP}(-\Phi, x)$ has $p(x) - \mathrm{i}p_{\mathrm{Im}}(x)$ in its top-left corner. So, using LCU, we can average these two to get a block-encoding of $p(x)$.

2.2 Lifting with the CS decomposition

To generalize to higher dimensions, we need a new version of QSP (Definition 2.1). In this discussion, we follow the exposition of [TT23].

Definition 2.6 ([GSLW19, Definition 15])**.** The *phased alternating sequence* associated with a partitioned unitary U (following notation of Definition 1.1) and $\Phi = \{\phi_j\}_{j \in [n]} \in \mathbb{R}^n$ is

$$U_\Phi \coloneqq \begin{cases} e^{\mathrm{i}\phi_1(2\Pi_{\mathrm{L}} - I)} U \prod_{j \in [\frac{n-1}{2}]} e^{\mathrm{i}\phi_{2j}(2\Pi_{\mathrm{R}} - I)} U^\dagger e^{\mathrm{i}\phi_{2j+1}(2\Pi_{\mathrm{L}} - I)} U & \text{if } n \text{ is odd, and} \\ \prod_{j \in [\frac{n}{2}]} e^{\mathrm{i}\phi_{2j-1}(2\Pi_{\mathrm{R}} - I)} U^\dagger e^{\mathrm{i}\phi_{2j}(2\Pi_{\mathrm{L}} - I)} U & \text{if } n \text{ is even.} \end{cases}$$

Remark 2.7. The phased alternating sequence U_Φ can be seen as a generalization of the quantum signal processing circuit $\mathbf{QSP}(\Phi, x)$. When $d = 2$ and $r = c = 1$, $2\Pi_{\mathrm{L}} - I =$

$2\Pi_{\mathrm{R}} - I = \sigma_z$, so

$$\mathbf{QSP}(\Phi, x) = [R(x)]_\Phi \text{ where } R(x) = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}.$$

Theorem 2.8 ([GSLW19, Theorem 17])**.** *Let unitary $U \in \mathbb{C}^{d\times d}$ be a Q-block encoding of A. Suppose $\Phi = \{\phi_j\}_{j\in[n]} \in \mathbb{R}^n$ is such that $\mathbf{QSP}(\Phi, x)$ computes the degree-n polynomial $p(x) \in \mathbb{C}[x]$, as in Definition 2.1. Then, U_Φ is a $d(\log(d) + Q)$-block encoding of $p^{(\mathrm{SV})}(A)$.*

We begin by proving the existence of the CS decomposition (CSD), a decomposition of a partitioned unitary matrix, following Paige and Wei [PW94].

The main idea of the CSD is that when a unitary matrix U is split into two-by-two blocks U_{ij} for $i, j \in \{1, 2\}$, one can produce "simultaneous singular value decompositions (SVDs)" of the blocks, of the form $U_{ij} = V_i D_{ij} W_j^\dagger$.[2]

Theorem 2.9. *Let $U \in \mathbb{C}^{d\times d}$ be a unitary matrix, partitioned into blocks of size $\{r_1, r_2\} \times \{c_1, c_2\}$:*

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}, \text{ where } U_{ij} \in \mathbb{C}^{r_i \times c_j} \text{ for } i, j \in \{1, 2\}.$$

Then, there exists unitary $V_i \in \mathbb{C}^{r_i\times r_i}$ and $W_j \in \mathbb{C}^{c_j\times c_j}$ for $i, j \in \{1, 2\}$ such that

$$\begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} \begin{pmatrix} W_1 & \\ & W_2 \end{pmatrix}^\dagger,$$

where blanks represent zero matrices and $D_{ij} \in \mathbb{R}^{r_i\times c_j}$ are diagonal matrices, possibly padded with zero rows or columns. Specifically, we can write

$$D := \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix} = \left(\begin{array}{ccc|ccc} 0 & & & I & & \\ & C & & & S & \\ & & I & & & 0 \\ \hline I & & & 0 & & \\ & S & & & -C & \\ & & 0 & & & -I \end{array}\right) \tag{24}$$

where I, C, and S blocks are square diagonal matrices where C and S have entries in $(0, 1)$ on the diagonal, and 0 blocks may be rectangular.[3] *Because D is unitary, we also have $C^2 + S^2 = I$.*

Remark 2.10. The form of D naturally induces decompositions $\mathbb{C}^d = \mathcal{X}_0 \oplus \mathcal{X}_C \oplus \mathcal{X}_1$ and $\mathbb{C}^d = \mathcal{Y}_0 \oplus \mathcal{Y}_C \oplus \mathcal{Y}_1$ into direct sums of three spaces. Hence, $D : \mathbb{C}^d \to \mathbb{C}^d$ can be seen as a map $D : \mathcal{X}_0 \oplus \mathcal{X}_C \oplus \mathcal{X}_1 \to \mathcal{Y}_0 \oplus \mathcal{Y}_C \oplus \mathcal{Y}_1$, such that D is a direct sum of three linear maps.

$$\left(\begin{array}{ccc|ccc} 0 & & & I & & \\ & C & & & S & \\ & & I & & & 0 \\ \hline I & & & 0 & & \\ & S & & & -C & \\ & & 0 & & & -I \end{array}\right) = \underbrace{\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}}_{\mathcal{X}_0 \to \mathcal{Y}_0} \oplus \underbrace{\begin{pmatrix} C & S \\ S & -C \end{pmatrix}}_{\mathcal{X}_C \to \mathcal{Y}_C} \oplus \underbrace{\begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}}_{\mathcal{X}_1 \to \mathcal{Y}_1}.$$

[2] In fact, there is some sense in which the SVD and the CSD are special cases of the same object, a *generalized Cartan decomposition*. We recommend the survey by Edelman and Jeong for readers curious about this connection [EJ21].

[3] Blocks may be non-existent. The I blocks may not necessarily be the same size, but C and S are the same size.

The key resulting intuition for QSVT is that, supposing everything is square, these blocks can be further decomposed into 2×2 blocks of the following rotation matrix form

$$\begin{pmatrix} \lambda_i & \sqrt{1-\lambda_i^2} \\ \sqrt{1-\lambda_i^2} & -\lambda_i \end{pmatrix}$$

from this representation, where $\{\lambda_i\}$ are the singular values of U_{11} (see Lemma 2.13).

2.3 Proving QSVT

We now apply the machinery of Section 2.2 to prove correctness of the QSVT framework of [GSLW19]. We begin with some helpful notation in this special case, following the partitioning given by Theorem 2.9.

Definition 2.11 (Variant of [GSLW19, Definition 12])**.** Let $U \in \mathbb{C}^{d \times d}$ be a Q-block encoding of $A \in \mathbb{C}^{r \times c}$ where $B_{\mathrm{L},1}$ and $B_{\mathrm{R},1}$ are the first r and c columns of the identity, respectively, as in Definition 1.1. By Theorem 2.9, there is a CS decomposition compatible with the partitioning of U:

$$U = \begin{pmatrix} A & U_{12} \\ U_{21} & U_{22} \end{pmatrix} = \underbrace{\begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix}}_{V} \underbrace{\begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} W_1 & \\ & W_2 \end{pmatrix}^\dagger}_{W^\dagger}.$$

In Definition 2.11, we applied Theorem 2.9 to obtain an SVD of $A = V_1 D_{11} W_1$ that we have extended to the d-dimensional U. Throughout the remainder of this section, $B_{\mathrm{L}}, B_{\mathrm{R}}, \Pi_{\mathrm{L}}$, and Π_{R} are defined consistently with the choice of $B_{\mathrm{L},1}$ and $B_{\mathrm{R},1}$ in Definition 2.11: $B_{\mathrm{L}} = B_{\mathrm{R}} = I$, and Π_{L} and Π_{R} are the identity but with all but the first r and c 1's set to 0, respectively. We next observe that this SVD commutes appropriately with exponentiated projections respecting the partition.

Lemma 2.12 (Variant of [GSLW19, Lemma 14])**.** *Let $\phi \in \mathbb{R}$. Following notation of Definition 2.11,*

$$e^{\mathrm{i}\phi(2\Pi_{\mathrm{L}} - I)} = \begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix}, \; e^{\mathrm{i}\phi(2\Pi_{\mathrm{R}} - I)} = \begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix},$$

with appropriate block sizes, and

$$\begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix} \begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} = \begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} \begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix},$$
$$\begin{pmatrix} W_1 & \\ & W_2 \end{pmatrix} \begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix} = \begin{pmatrix} e^{\mathrm{i}\phi} I & \\ & e^{-\mathrm{i}\phi} I \end{pmatrix} \begin{pmatrix} W_1 & \\ & W_2 \end{pmatrix}.$$

We next state our main technical claim, whose proof is deferred to the end of the section.

Lemma 2.13. *Consider $U \in \mathbb{C}^{d \times d}$ as a block matrix. Let $\Phi \in \mathbb{R}^n$ be the sequence of angles implementing the degree-n polynomial $p(x) \in \mathbb{C}[x]$ via quantum signal processing (Definition 2.1).*

1. *When $U = \begin{pmatrix} 0^{r \times c} & I_r \\ I_c & 0^{c \times r} \end{pmatrix}$, we have*

$$U_\Phi = \begin{pmatrix} p(0) I_c & \cdot \\ \cdot & \cdot \end{pmatrix} \text{ for } n \text{ even, and } U_\Phi = \begin{pmatrix} 0^{r \times c} & \cdot \\ \cdot & \cdot \end{pmatrix} \text{ for } n \text{ odd.} \tag{25}$$

2. *When* $U = \begin{pmatrix} I_r & 0^{r\times c} \\ 0^{c\times r} & -I_c \end{pmatrix}$, *we have*

$$U_\Phi = \begin{pmatrix} p(1)I_r & \cdot \\ \cdot & \cdot \end{pmatrix}. \tag{26}$$

3. *Let* $C, S \in \mathbb{C}^{r\times r}$ *be diagonal with* $C^2 + S^2 = I$. *Then when* $U = \begin{pmatrix} C & S \\ S & -C \end{pmatrix}$, *we have*

$$U_\Phi = \begin{pmatrix} p^{(\mathrm{SV})}(C) & \cdot \\ \cdot & \cdot \end{pmatrix}. \tag{27}$$

Using this lemma, our main QSVT result (Theorem 2.8) in the setting of Definition 2.11 follows directly.

Proof of Theorem 2.8, special case. For convenience, we recall the definition of U_Φ:

$$U_\Phi = \begin{cases} e^{\mathrm{i}\phi_1(2\Pi_\mathrm{L}-I)}U\prod_{j\in[\frac{n-1}{2}]} e^{\mathrm{i}\phi_{2j}(2\Pi_\mathrm{R}-I)}U^\dagger e^{\mathrm{i}\phi_{2j+1}(2\Pi_\mathrm{L}-I)}U & \text{if } n \text{ is odd, and} \\ \prod_{j\in[\frac{n}{2}]} e^{\mathrm{i}\phi_{2j-1}(2\Pi_\mathrm{R}-I)}U^\dagger e^{\mathrm{i}\phi_{2j}(2\Pi_\mathrm{L}-I)}U & \text{if } n \text{ is even.} \end{cases}$$

Using that V and $W^\dagger$ from the CS decomposition $U = VDW^\dagger$ commute with their adjacent exponentiated reflections (Lemma 2.12), we continue:

$$\begin{aligned} &= \begin{cases} Ve^{\mathrm{i}\phi_1(2\Pi_\mathrm{L}-I)}D(\prod_{j\in[\frac{n-1}{2}]} e^{\mathrm{i}\phi_{2j}(2\Pi_\mathrm{R}-I)}D^\dagger e^{\mathrm{i}\phi_{2j+1}(2\Pi_\mathrm{L}-I)}D)W^\dagger & \text{if } n \text{ is odd, and} \\ W(\prod_{j\in[\frac{n}{2}]} e^{\mathrm{i}\phi_{2j-1}(2\Pi_\mathrm{R}-I)}D^\dagger e^{\mathrm{i}\phi_{2j}(2\Pi_\mathrm{L}-I)}D)W^\dagger & \text{if } n \text{ is even} \end{cases} \\ &= \begin{cases} VD_\Phi W^\dagger & \text{if } n \text{ is odd, and} \\ WD_\Phi W^\dagger & \text{if } n \text{ is even.} \end{cases} \end{aligned} \tag{28}$$

This reduces the problem to computing D_Φ. Recall from (24) that the structure of D is

$$\left(\begin{array}{c|c} D_{11} & D_{12} \\ \hline D_{21} & D_{22} \end{array}\right) = \left(\begin{array}{ccc|ccc} 0 & & & I & & \\ & C & & & S & \\ & & I & & & 0 \\ \hline I & & & 0 & & \\ & S & & & -C & \\ & & 0 & & & -I \end{array}\right) = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \oplus \begin{pmatrix} C & S \\ S & -C \end{pmatrix} \oplus \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}.$$

Similarly, where the blocks below denote the same direct sum decomposition above, for $\phi \in \mathbb{R}$,

$$\begin{aligned} e^{\mathrm{i}\phi(2\Pi_\mathrm{L}-I)} &= \left(\begin{array}{c|c} e^{\mathrm{i}\phi}I & \\ \hline & e^{-\mathrm{i}\phi}I \end{array}\right) = \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix} \oplus \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix} \oplus \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix}, \\ e^{\mathrm{i}\phi(2\Pi_\mathrm{R}-I)} &= \left(\begin{array}{c|c} e^{\mathrm{i}\phi}I & \\ \hline & e^{-\mathrm{i}\phi}I \end{array}\right) = \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix} \oplus \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix} \oplus \begin{pmatrix} e^{\mathrm{i}\phi}I & \\ & e^{-\mathrm{i}\phi}I \end{pmatrix}. \end{aligned}$$

Leveraging this direct sum decomposition of D, applying Lemma 2.13 to each block yields

$$D_\Phi = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}_\Phi \oplus \begin{pmatrix} C & S \\ S & -C \end{pmatrix}_\Phi \oplus \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}_\Phi$$
$$= \begin{cases} \begin{pmatrix} 0 & \cdot \\ \cdot & \cdot \end{pmatrix} \oplus \begin{pmatrix} p^{(\mathrm{SV})}(C) & \cdot \\ \cdot & \cdot \end{pmatrix} \oplus \begin{pmatrix} p(1)I & \cdot \\ \cdot & \cdot \end{pmatrix} & \text{if } n \text{ is odd, and} \\ \begin{pmatrix} p(0)I & \cdot \\ \cdot & \cdot \end{pmatrix} \oplus \begin{pmatrix} p^{(\mathrm{SV})}(C) & \cdot \\ \cdot & \cdot \end{pmatrix} \oplus \begin{pmatrix} p(1)I & \cdot \\ \cdot & \cdot \end{pmatrix} & \text{if } n \text{ is even.} \end{cases}$$

So, for n odd, recalling (28) and $p(0) = 0$, we have

$$\Pi_{\mathrm{L}} U_\Phi \Pi_{\mathrm{R}} = \Pi_{\mathrm{L}} V D_\Phi W^\dagger \Pi_{\mathrm{R}}$$
$$= \begin{pmatrix} I & \end{pmatrix} \begin{pmatrix} V_1 & \\ & V_2 \end{pmatrix} D_\Phi \begin{pmatrix} W_1^\dagger & \\ & W_2^\dagger \end{pmatrix} \begin{pmatrix} I & \end{pmatrix} = \begin{pmatrix} V_1 & \end{pmatrix} D_\Phi \begin{pmatrix} W_1^\dagger & \end{pmatrix}$$
$$= \left(\begin{array}{c|c} V_1 \begin{pmatrix} 0 & & \\ & p^{(\mathrm{SV})}(C) & \\ & & p(1)I \end{pmatrix} W_1^\dagger & \\ \hline & \end{array}\right) = \left(\begin{array}{c|c} p^{(\mathrm{SV})}(A) & 0 \\ \hline 0 & 0 \end{array}\right).$$

Similarly, for n even, we have

$$\Pi_{\mathrm{R}} U_\Phi \Pi_{\mathrm{R}} = \Pi_{\mathrm{R}} W D_\Phi W^\dagger \Pi_{\mathrm{R}}$$
$$= \begin{pmatrix} W_1 & \end{pmatrix} D_\Phi \begin{pmatrix} W_1^\dagger & \end{pmatrix}$$
$$= \left(\begin{array}{c|c} W_1 \begin{pmatrix} p(0)I & & \\ & p^{(\mathrm{SV})}(C) & \\ & & p(1)I \end{pmatrix} W_1^\dagger & \\ \hline & \end{array}\right) = \left(\begin{array}{c|c} p^{(\mathrm{SV})}(A) & 0 \\ \hline 0 & 0 \end{array}\right).$$

□

We conclude the section by proving Lemma 2.13.

Proof of Lemma 2.13. The basic intuition behind this argument is that, by assumption and (3),

$$\prod_{j \in [n]} \begin{pmatrix} e^{\mathrm{i}\phi_j} & 0 \\ 0 & e^{-\mathrm{i}\phi_j} \end{pmatrix} \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} = \begin{pmatrix} p(x) & \cdot \\ \cdot & \cdot \end{pmatrix}.$$

So, supposing we could evaluate the polynomial at a matrix $x \leftarrow C$, we get that

$$\text{“} \prod_{j \in [n]} \begin{pmatrix} e^{\mathrm{i}\phi_j} I & 0 \\ 0 & e^{-\mathrm{i}\phi_j} I \end{pmatrix} \begin{pmatrix} C & \sqrt{I-C^2} \\ \sqrt{I-C^2} & -C \end{pmatrix} = \begin{pmatrix} p(C) & \cdot \\ \cdot & \cdot \end{pmatrix}.\text{”}$$

This should hold because block matrix multiplication operates by the same rules as scalar matrix multiplication, but requires care to handle the non-square case. Here, we handle this in a more elementary manner. First, we consider (25). When n is even,

$$\begin{aligned} U_\Phi &= \prod_{j\in[\frac{n}{2}]} \begin{pmatrix} e^{\mathrm{i}\phi_{2j-1}} I & \\ & e^{-\mathrm{i}\phi_{2j-1}} I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}^\dagger \begin{pmatrix} e^{\mathrm{i}\phi_{2j}} I & \\ & e^{-\mathrm{i}\phi_{2j}} I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \\ &= \prod_{j\in[\frac{n}{2}]} \begin{pmatrix} e^{\mathrm{i}(\phi_{2j-1}-\phi_{2j})} I & 0 \\ 0 & e^{-\mathrm{i}(\phi_{2j-1}-\phi_{2j})} I \end{pmatrix} = \begin{pmatrix} e^{\mathrm{i}\sum_{k\in[n]}(-1)^{k+1}\phi_k} I & 0 \\ 0 & e^{-\mathrm{i}\sum_{k\in[n]}(-1)^{k+1}\phi_k} I \end{pmatrix}. \end{aligned}$$

Taking I and 0 to be 1-dimensional scalars 1 and 0, this computation and Definition 2.1 also show that $p(0) = e^{\mathrm{i}\sum_{k\in[n]}(-1)^{k+1}\phi_k}$ yielding the desired conclusion. Similarly, when n is odd,

$$\begin{aligned} U_\Phi &= \begin{pmatrix} e^{\mathrm{i}\phi_1} I & \\ & e^{-\mathrm{i}\phi_1} I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \prod_{j\in[\frac{n-1}{2}]} \begin{pmatrix} e^{\mathrm{i}\phi_{2j}} I & \\ & e^{-\mathrm{i}\phi_{2j}} I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}^\dagger \begin{pmatrix} e^{\mathrm{i}\phi_{2j+1}} I & \\ & e^{-\mathrm{i}\phi_{2j+1}} I \end{pmatrix} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & e^{\mathrm{i}\sum_{k\in[n]}(-1)^{k+1}\phi_k} I \\ e^{-\mathrm{i}\sum_{k\in[n]}(-1)^{k+1}\phi_k} I & 0 \end{pmatrix}. \end{aligned}$$

Next, we prove (26). Since U is a real diagonal matrix, it is Hermitian and commutes with the other matrices in the expression U_Φ. As an immediate consequence,

$$U_\Phi = \begin{pmatrix} I & 0 \\ 0 & (-1)^n I \end{pmatrix} \prod_{k\in[n]} \begin{pmatrix} e^{\mathrm{i}\phi_k} I & 0 \\ 0 & e^{-\mathrm{i}\phi_k} I \end{pmatrix} = \begin{pmatrix} e^{\mathrm{i}\sum_{k\in[n]}\phi_k} I & 0 \\ 0 & (-1)^n e^{-\mathrm{i}\sum_{k\in[n]}\phi_k} I \end{pmatrix}.$$

As before, the same computation specialized to a 2-dimensional $U = \sigma_z$ shows that $p(1) = e^{\mathrm{i}\sum_{k\in[n]}\phi_k}$ giving the desired claim. Finally to prove (27), let the diagonal entries of C be $\{c_i\}_{i\in[r]}$. Then, U is the direct sum of r matrices of the form $R(c_i)$, where we recall we defined R in Definition 2.1. Applying Definition 2.1 to each 2×2 block, and comparing to the definition of $p^{(\mathrm{SV})}(A)$, yields the conclusion. □

References

[EJ21] Alan Edelman and Sungwoo Jeong. *Fifty three matrix factorizations: a systematic approach*. 2021. DOI: 10.48550/ARXIV.2104.08669 (page 5).

[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 (pages 1, 2, 4–6).

[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 1).

[PW94] C. C. Paige and M. Wei. "History and generality of the CS decomposition". In: *Linear Algebra and Its Applications* 208/209 (1994), pp. 303–326. ISSN: 0024-3795. DOI: 10.1016/0024-3795(94)90446-4 (page 5).

[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 1).

[TT23] Ewin Tang and Kevin Tian. *A CS guide to the quantum singular value transformation*. 2023. arXiv: 2302.14324 [quant-ph] (page 4).