A CS guide to the quantum singular value transformation

Ewin Tang
UC Berkeley

Kevin Tian
UT Austin

arXiv:2302.14324

Motivation

arXiv.org > quant-ph > arXiv:2105.02859

Quantum Physics

[Submitted on 6 May 2021 (v1), last revised 20 Aug 2021 (this version, v3)]

A Grand Unification of Quantum Algorithms

John M. Martyn, Zane M. Rossi, Andrew K. Tan, Isaac L. Chuang

QSVT is a single framework comprising the three major quantum algorithms [Shor's algorithm, Grover's algorithm, and Hamiltonian simulation], thus suggesting a grand unification of quantum algorithms.

Summary

QSVT is now a dominant paradigm for quantum algorithm design.

The framework is laid out in greatest generality in [GSLW18].[1]

We present two simplifications of it.

[1] Gilyén, Su, Low, Wiebe – *Quantum singular value transformation and beyond*

Summary

QSVT is now a dominant paradigm for quantum algorithm design.

The framework is laid out in greatest generality in [GSLW18].[1]

We present two simplifications of it.

1. Streamline the proof of the “main theorem” via the Cosine-Sine decomposition

[1] Gilyén, Su, Low, Wiebe – *Quantum singular value transformation and beyond*

Summary

QSVT is now a dominant paradigm for quantum algorithm design.

The framework is laid out in greatest generality in [GSLW18].[1]

We present two simplifications of it.

1. Streamline the proof of the “main theorem” via the Cosine-Sine decomposition
2. Streamline applications of the “main theorem” via Chebyshev Series

[1] Gilyén, Su, Low, Wiebe – *Quantum singular value transformation and beyond*

Background

Primer: A dictionary for quantum terms

quantum state on q qubits	unit vector $v \in \mathbb{C}^{2^q}$
quantum gate/circuit on q qubits	unitary[2] matrix $\mathbf{U} \in \mathbb{C}^{2^q \times 2^q}$.
"efficient" circuit on q qubits	a product $\prod_i \mathbf{V}_i$ of $\mathrm{poly}(q)$ elementary unitaries.

[2] U is unitary when its conjugate transpose $U^\dagger$ equals its inverse U^{-1}.

The primitive of the block-encoding

Definition (Block-encoding)

We say that a unitary $\mathbf{U} \in \mathbb{C}^{d\times d}$ is a *block encoding* of the matrix $\mathbf{A} \in \mathbb{C}^{r\times c}$ if

$$\mathbf{U} = \begin{pmatrix} \mathbf{A} & \cdot \\ \cdot & \cdot \end{pmatrix} \iff \mathbf{\Pi}_{\mathsf{L}} \mathbf{U} \mathbf{\Pi}_{\mathsf{R}} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

This implies that $\|\mathbf{A}\| \leq 1$.

The primitive of the block-encoding

Definition (Block-encoding)

We say that a unitary $\mathbf{U} \in \mathbb{C}^{d\times d}$ is a *block encoding* of the matrix $\mathbf{A} \in \mathbb{C}^{r\times c}$ if

$$\mathbf{U} = \begin{pmatrix} \mathbf{A} & \cdot \\ \cdot & \cdot \end{pmatrix} \iff \mathbf{\Pi}_{\mathsf{L}}\mathbf{U}\mathbf{\Pi}_{\mathsf{R}} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

This implies that $\|\mathbf{A}\| \leq 1$.

We want *efficient* block-encodings, i.e. $\mathbf{U}$ with $\mathrm{poly}\log(rc)$-sized quantum circuits.

Block-encodings from sparsity

If $\mathbf{A}$ is s-row-sparse and s-column sparse, with entries bounded by 1, we have an efficient block-encoding to $\mathbf{A}/s$.

The fundamental theorem of block-encodings

Definition (Singular value transformation)

For an even or odd, degree-n polynomial p and a matrix $\mathbf{A} \in \mathbb{C}^{r \times c}$, $p^{\text{(SV)}}(\mathbf{A})$ is the linear extension of the map

$$p(x) = x^{2k} \implies p^{\text{(SV)}}(\mathbf{A}) = (\mathbf{A}\mathbf{A}^\dagger)^k$$
$$p(x) = x^{2k+1} \implies p^{\text{(SV)}}(\mathbf{A}) = (\mathbf{A}\mathbf{A}^\dagger)^k\mathbf{A}$$

This is basically applying p to the singular values of $\mathbf{A}$.

The fundamental theorem of block-encodings

Definition (Singular value transformation)

For an even or odd, degree-n polynomial p and a matrix $\mathbf{A} \in \mathbb{C}^{r \times c}$, $p^{\text{(SV)}}(\mathbf{A})$ is the linear extension of the map

$$p(x) = x^{2k} \implies p^{\text{(SV)}}(\mathbf{A}) = (\mathbf{A}\mathbf{A}^\dagger)^k$$
$$p(x) = x^{2k+1} \implies p^{\text{(SV)}}(\mathbf{A}) = (\mathbf{A}\mathbf{A}^\dagger)^k \mathbf{A}$$

Theorem (Quantum singular value transformation)

Given a block-encoding of $\mathbf{A}$, we can get a block-encoding of $p^{\text{(SV)}}(\mathbf{A})$, where p is an even or odd degree-n polynomial satisfying

$$\max_{x \in [-1,1]} |p(x)| \leq 1.$$

The quantum circuit implementing $p^{\text{(SV)}}(\mathbf{A})$ becomes larger by only a factor of n.

Proof of the fundamental theorem

The scalar case

Definition (Quantum signal processing)

A sequence of phase factors $\Phi = \{\phi_j\}_{0\le j\le n} \in \mathbb{R}^{n+1}$ defines a *quantum signal processing* circuit

$$\mathbf{QSP}(\Phi, x) \coloneqq \mathbf{Z}(\phi_0)\mathbf{R}(x)\mathbf{Z}(\phi_1)\dots\mathbf{Z}(\phi_{n-1})\mathbf{R}(x)\mathbf{Z}(\phi_n)$$

where

$$\mathbf{Z}(\phi) = e^{\mathrm{i}\phi\boldsymbol{\sigma}_z} = \begin{pmatrix} e^{\mathrm{i}\phi} & 0 \\ 0 & e^{-\mathrm{i}\phi} \end{pmatrix}, \qquad \mathbf{R}(x) = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}$$

The scalar case

Definition (Quantum signal processing)

A sequence of phase factors $\Phi = \{\phi_j\}_{0\le j\le n} \in \mathbb{R}^{n+1}$ defines a *quantum signal processing* circuit

$$\mathbf{QSP}(\Phi, x) \coloneqq \mathbf{Z}(\phi_0)\mathbf{R}(x)\mathbf{Z}(\phi_1)\ldots\mathbf{Z}(\phi_{n-1})\mathbf{R}(x)\mathbf{Z}(\phi_n)$$

where

$$\mathbf{Z}(\phi) = e^{\mathrm{i}\phi\boldsymbol{\sigma}_z} = \begin{pmatrix} e^{\mathrm{i}\phi} & 0 \\ 0 & e^{-\mathrm{i}\phi} \end{pmatrix}, \qquad \mathbf{R}(x) = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}$$

For every odd or even, degree-n, bounded p, there is a $\Phi \in \mathbb{R}^{n+1}$ such that*

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

The general case

Definition (Phased alternating sequence)

For a block-encoding $\mathbf{U}$ and $\Phi = \{\phi_j\}_{0 \leq j \leq n} \in \mathbb{R}^{n+1}$, let

$$\mathbf{U}_\Phi := \begin{cases} \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1) \prod_{j=1}^{\frac{n-1}{2}} \mathbf{U}^\dagger \mathbf{Z}_{\mathsf{L}}(\phi_{2j})\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_{2j+1}) & \text{if } n \text{ is odd, and} \\ \mathbf{Z}_{\mathsf{R}}(\phi_0) \prod_{j=1}^{\frac{n}{2}} \mathbf{U}^\dagger \mathbf{Z}_{\mathsf{L}}(\phi_{2j-1})\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_{2j}) & \text{if } n \text{ is even.} \end{cases}$$

$$\mathbf{Z}_{\mathsf{L}}(\phi) = \begin{pmatrix} e^{\mathrm{i}\phi}\mathbf{I}_r & \\ & e^{-\mathrm{i}\phi}\mathbf{I}_{d-r} \end{pmatrix}, \; \mathbf{Z}_{\mathsf{R}}(\phi) = \begin{pmatrix} e^{\mathrm{i}\phi}\mathbf{I}_c & \\ & e^{-\mathrm{i}\phi}\mathbf{I}_{d-c} \end{pmatrix},$$

$$\mathbf{U} = \begin{pmatrix} \mathbf{A} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{pmatrix}$$

The fundamental theorem, restated

Theorem

Let the unitary $\mathbf{U} \in \mathbb{C}^{d\times d}$ be a block encoding of $\mathbf{A}$. Let $\Phi = \{\phi_j\}_{0\le j\le n} \in \mathbb{R}^{n+1}$ be the sequence of phase factors such that $\mathbf{QSP}(\Phi, x)$ computes the degree-n polynomial $p(x)$. Then $\mathbf{U}_\Phi$ is a block encoding of $p^{\text{(SV)}}(\mathbf{A})$:

$$\text{if } p \text{ is odd,} \quad \mathbf{\Pi}_{\text{L}}\mathbf{U}_\Phi\mathbf{\Pi}_{\text{R}} = \begin{pmatrix} p^{\text{(SV)}}(\mathbf{A}) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix},$$

$$\text{and if } p \text{ is even,} \quad \mathbf{\Pi}_{\text{R}}\mathbf{U}_\Phi\mathbf{\Pi}_{\text{R}} = \begin{pmatrix} p^{\text{(SV)}}(\mathbf{A}) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

The cosine-sine decomposition

- Introduced by Davis and Kahan in 1969
- Strengthened work by Jordan on angles between subspaces (Jordan's lemma, 1875)
- Named and championed by Stewart

> *Briefly, whenever some aspect of a problem can be usefully formulated in terms of two-block by two-block partitions of unitary matrices, the CS decomposition will probably add insights and simplify the analysis.*
>
> *—Paige and Wei*

The cosine-sine decomposition

Let $\mathbf{U} \in \mathbb{C}^{d\times d}$ be a 2×2 block matrix which is unitary. Then there exist unitaries $\mathbf{V}_i \in \mathbb{C}^{r_i \times r_i}$ and $\mathbf{W}_j \in \mathbb{C}^{c_j \times c_j}$ giving simultaneous SVDs for all blocks of $\mathbf{U}$:

$$\begin{pmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{pmatrix} = \begin{pmatrix} \mathbf{V}_1 & \\ & \mathbf{V}_2 \end{pmatrix} \begin{pmatrix} \mathbf{D}_{11} & \mathbf{D}_{12} \\ \mathbf{D}_{21} & \mathbf{D}_{22} \end{pmatrix} \begin{pmatrix} \mathbf{W}_1 & \\ & \mathbf{W}_2 \end{pmatrix}^\dagger .$$

For example, $\mathbf{U}_{12} = \mathbf{V}_1 \mathbf{D}_{12} \mathbf{W}_2^\dagger$.

The cosine-sine decomposition

Let $\mathbf{U} \in \mathbb{C}^{d\times d}$ be a 2×2 block matrix which is unitary. Then there exist unitaries $\mathbf{V}_i \in \mathbb{C}^{r_i\times r_i}$ and $\mathbf{W}_j \in \mathbb{C}^{c_j\times c_j}$ giving simultaneous SVDs for all blocks of $\mathbf{U}$:

$$\begin{pmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{pmatrix} = \begin{pmatrix} \mathbf{V}_1 & \\ & \mathbf{V}_2 \end{pmatrix} \begin{pmatrix} \mathbf{D}_{11} & \mathbf{D}_{12} \\ \mathbf{D}_{21} & \mathbf{D}_{22} \end{pmatrix} \begin{pmatrix} \mathbf{W}_1 & \\ & \mathbf{W}_2 \end{pmatrix}^\dagger.$$

For example, $\mathbf{U}_{12} = \mathbf{V}_1\mathbf{D}_{12}\mathbf{W}_2^\dagger$.

$$\mathbf{D} := \left(\begin{array}{ccc|ccc} \mathbf{0} & & & \mathbf{I} & & \\ & \mathbf{C} & & & \mathbf{S} & \\ & & \mathbf{I} & & & \mathbf{0} \\ \hline \mathbf{I} & & & \mathbf{0} & & \\ & \mathbf{S} & & & -\mathbf{C} & \\ & & \mathbf{0} & & & -\mathbf{I} \end{array}\right) = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{pmatrix} \oplus \begin{pmatrix} \mathbf{C} & \mathbf{S} \\ \mathbf{S} & -\mathbf{C} \end{pmatrix} \oplus \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & -\mathbf{I} \end{pmatrix}.$$

Proof sketch, for $n = 3$

$$\mathbf{U}_{\Phi} = \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^{\dagger}\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3)$$

Proof sketch, for $n = 3$

$$\mathbf{U}_\Phi = \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3)$$

We consider a CS decomposition compatible with the partitioning of $\mathbf{U}$:

$$\mathbf{U} = \begin{pmatrix} \mathbf{A} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{V}_1 & \\ & \mathbf{V}_2 \end{pmatrix}}_{\mathbf{V}} \underbrace{\begin{pmatrix} \mathbf{D}_{11} & \mathbf{D}_{12} \\ \mathbf{D}_{21} & \mathbf{D}_{22} \end{pmatrix}}_{\mathbf{D}} \underbrace{\begin{pmatrix} \mathbf{W}_1 & \\ & \mathbf{W}_2 \end{pmatrix}^\dagger}_{\mathbf{W}^\dagger}.$$

Proof sketch, for $n = 3$

$$\begin{aligned}
\mathbf{U}_\Phi &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3) \\
&= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{W}\mathbf{D}^\dagger\mathbf{V}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_3)
\end{aligned}$$

Proof sketch, for $n = 3$

$$\begin{aligned}\mathbf{U}_\Phi &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3) \\ &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{W}\mathbf{D}^\dagger\mathbf{V}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_3)\end{aligned}$$

$\mathbf{Z}_{\mathsf{L}}$ and $\mathbf{V}$ commute; $\mathbf{Z}_{\mathsf{R}}$ and $\mathbf{W}$ commute;

$$\begin{pmatrix} e^{i\phi}\mathbf{I} & \\ & e^{-i\phi}\mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{V}_1 & \\ & \mathbf{V}_2\end{pmatrix} = \begin{pmatrix}\mathbf{V}_1 & \\ & \mathbf{V}_2\end{pmatrix}\begin{pmatrix} e^{i\phi}\mathbf{I} & \\ & e^{-i\phi}\mathbf{I}\end{pmatrix},$$

$$\begin{pmatrix}\mathbf{W}_1 & \\ & \mathbf{W}_2\end{pmatrix}\begin{pmatrix} e^{i\phi}\mathbf{I} & \\ & e^{-i\phi}\mathbf{I}\end{pmatrix} = \begin{pmatrix} e^{i\phi}\mathbf{I} & \\ & e^{-i\phi}\mathbf{I}\end{pmatrix}\begin{pmatrix}\mathbf{W}_1 & \\ & \mathbf{W}_2\end{pmatrix}.$$

Proof sketch, for $n = 3$

$$
\begin{aligned}
\mathbf{U}_\Phi &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3) \\
&= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{W}\mathbf{D}^\dagger\mathbf{V}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_3) \\
&= \mathbf{V}\Big(\mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{D}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{D}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{D}\mathbf{Z}_{\mathsf{R}}(\phi_3)\Big)\mathbf{W}^\dagger \\
&= \mathbf{V}\mathbf{D}_\Phi\mathbf{W}^\dagger
\end{aligned}
$$

Proof sketch, for $n = 3$

$$\begin{aligned}\mathbf{U}_\Phi &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{U}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{U}\mathbf{Z}_{\mathsf{R}}(\phi_3)\\ &= \mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{W}\mathbf{D}^\dagger\mathbf{V}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{V}\mathbf{D}\mathbf{W}^\dagger\mathbf{Z}_{\mathsf{R}}(\phi_3)\\ &= \mathbf{V}\Big(\mathbf{Z}_{\mathsf{L}}(\phi_0)\mathbf{D}\mathbf{Z}_{\mathsf{R}}(\phi_1)\mathbf{D}^\dagger\mathbf{Z}_{\mathsf{L}}(\phi_2)\mathbf{D}\mathbf{Z}_{\mathsf{R}}(\phi_3)\Big)\mathbf{W}^\dagger\\ &= \mathbf{V}\mathbf{D}_\Phi\mathbf{W}^\dagger\end{aligned}$$

This reduces the problem to computing $\mathbf{D}_\Phi$. Recall that

$$\mathbf{D} = \begin{pmatrix}\mathbf{0} & \mathbf{I}\\ \mathbf{I} & \mathbf{0}\end{pmatrix} \oplus \begin{pmatrix}\mathbf{C} & \mathbf{S}\\ \mathbf{S} & -\mathbf{C}\end{pmatrix} \oplus \begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & -\mathbf{I}\end{pmatrix}.$$

Further, we have

$$\mathbf{D}_\Phi = \left[\begin{pmatrix}\mathbf{0} & \mathbf{I}\\ \mathbf{I} & \mathbf{0}\end{pmatrix}\right]_\Phi \oplus \left[\begin{pmatrix}\mathbf{C} & \mathbf{S}\\ \mathbf{S} & -\mathbf{C}\end{pmatrix}\right]_\Phi \oplus \left[\begin{pmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & -\mathbf{I}\end{pmatrix}\right]_\Phi$$

Proof sketch, for $n = 3$

Upon proving the statement for the individual cases, we get

$$\begin{aligned}
\mathbf{U}_\Phi &= \mathbf{V}\mathbf{D}_\Phi\mathbf{W}^\dagger \\
&= \begin{pmatrix} \mathbf{V}_1 & \\ & \mathbf{V}_2 \end{pmatrix} \begin{pmatrix} p^{(\mathsf{SV})}(\mathbf{D}_{11}) & \cdot \\ \cdot & \cdot \end{pmatrix} \begin{pmatrix} \mathbf{W}_1^\dagger & \\ & \mathbf{W}_2^\dagger \end{pmatrix} \\
&= \begin{pmatrix} \mathbf{V}_1 p^{(\mathsf{SV})}(\mathbf{D}_{11})\mathbf{W}_1^\dagger & \cdot \\ \cdot & \cdot \end{pmatrix} \\
&= \begin{pmatrix} p^{(\mathsf{SV})}(\mathbf{A}) & \cdot \\ \cdot & \cdot \end{pmatrix}
\end{aligned}$$

What we avoided

Lemma 14 (Invariant subspace decomposition of a projected unitary). *Let $\mathcal{H}_U$ be a finite-dimensional Hilbert-space and $U, \Pi, \widetilde{\Pi} \in \mathrm{End}(\mathcal{H}_U)$ be as in Definition 11. Then using the singular value decomposition of Definition 12 we have that*

$$U = \bigoplus_{i\in[k]} [\varsigma_i]_{\tilde{\mathcal{H}}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[r]\setminus[k]} \begin{bmatrix} \varsigma_i & \sqrt{1-\varsigma_i^2} \\ \sqrt{1-\varsigma_i^2} & -\varsigma_i \end{bmatrix}_{\tilde{\mathcal{H}}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[d]\setminus[r]} [1]_{\tilde{\mathcal{H}}_i^R}^{\mathcal{H}_i^R} \oplus \bigoplus_{i\in[\tilde{d}]\setminus[r]} [1]_{\tilde{\mathcal{H}}_i^L}^{\mathcal{H}_i^L} \oplus [\,\cdot\,]_{\tilde{\mathcal{H}}_\perp}^{\mathcal{H}_\perp}. \tag{24}$$

Moreover,

$$2\Pi - I = \bigoplus_{i\in[k]} [1]_{\mathcal{H}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[r]\setminus[k]} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}_{\mathcal{H}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[d]\setminus[r]} [1]_{\mathcal{H}_i^R}^{\mathcal{H}_i^R} \oplus \bigoplus_{i\in[d]\setminus[r]} [-1]_{\mathcal{H}_i^L}^{\mathcal{H}_i^L} \oplus [\,\cdot\,]_{\mathcal{H}_\perp}^{\mathcal{H}_\perp}, \tag{25}$$

$$e^{i\phi(2\Pi-I)} = \bigoplus_{i\in[k]} \left[e^{i\phi}\right]_{\mathcal{H}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[r]\setminus[k]} \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix}_{\mathcal{H}_i}^{\mathcal{H}_i} \oplus \bigoplus_{i\in[d]\setminus[r]} \left[e^{i\phi}\right]_{\mathcal{H}_i^R}^{\mathcal{H}_i^R} \oplus \bigoplus_{i\in[d]\setminus[r]} \left[e^{-i\phi}\right]_{\mathcal{H}_i^L}^{\mathcal{H}_i^L} \oplus [\,\cdot\,]_{\mathcal{H}_\perp}^{\mathcal{H}_\perp}, \tag{26}$$

and

$$2\widetilde{\Pi} - I = \bigoplus_{i\in[k]} [1]_{\tilde{\mathcal{H}}_i}^{\tilde{\mathcal{H}}_i} \oplus \bigoplus_{i\in[r]\setminus[k]} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}_{\tilde{\mathcal{H}}_i}^{\tilde{\mathcal{H}}_i} \oplus \bigoplus_{i\in[d]\setminus[r]} [-1]_{\tilde{\mathcal{H}}_i^R}^{\tilde{\mathcal{H}}_i^R} \oplus \bigoplus_{i\in[d]\setminus[r]} [1]_{\tilde{\mathcal{H}}_i^L}^{\tilde{\mathcal{H}}_i^L} \oplus [\,\cdot\,]_{\tilde{\mathcal{H}}_\perp}^{\tilde{\mathcal{H}}_\perp}, \tag{27}$$

$$e^{i\phi(2\widetilde{\Pi}-I)} = \bigoplus_{i\in[k]} \left[e^{i\phi}\right]_{\tilde{\mathcal{H}}_i}^{\tilde{\mathcal{H}}_i} \oplus \bigoplus_{i\in[r]\setminus[k]} \begin{bmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{bmatrix}_{\tilde{\mathcal{H}}_i}^{\tilde{\mathcal{H}}_i} \oplus \bigoplus_{i\in[d]\setminus[r]} \left[e^{-i\phi}\right]_{\tilde{\mathcal{H}}_i^R}^{\tilde{\mathcal{H}}_i^R} \oplus \bigoplus_{i\in[d]\setminus[r]} \left[e^{i\phi}\right]_{\tilde{\mathcal{H}}_i^L}^{\tilde{\mathcal{H}}_i^L} \oplus [\,\cdot\,]_{\tilde{\mathcal{H}}_\perp}^{\tilde{\mathcal{H}}_\perp}. \tag{28}$$

Applications of the fundamental theorem

Polynomial approximation for applications

In applications, we want a block-encoding of $f(\mathbf{A})$, so we compute an approximation $p^{(\mathsf{SV})}(\mathbf{A})$.

Application	$f(x)$	**Method of approximation**
Random walks	x^k	ad-hoc
Simulating Hamiltonians	$e^{\mathrm{i}xt}$	Chebyshev truncation
Solving linear systems	$1/x$	ad-hoc
Computing entropies	x^{-c}	Fourier truncation of Taylor truncation
Taking roots of unitaries	$\arcsin$	Fourier truncation of Taylor truncation

Polynomial approximation for applications

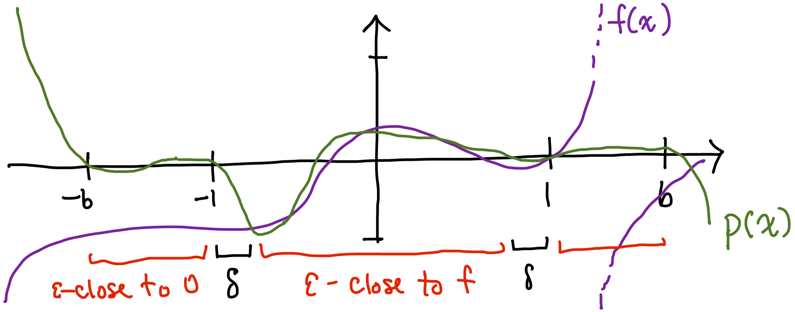
In applications, we want a block-encoding of $f(\mathbf{A})$, so we compute an approximation $p^{(\mathsf{SV})}(\mathbf{A})$.

Application	$f(x)$	Method of approximation
Random walks	x^k	ad-hoc
Simulating Hamiltonians	$e^{\mathrm{i}xt}$	Chebyshev truncation
Solving linear systems	$1/x$	ad-hoc
Computing entropies	x^{-c}	Fourier truncation of Taylor truncation
Taking roots of unitaries	$\arcsin$	Fourier truncation of Taylor truncation

We recover all the above up to a log, just using Chebyshev-based methods!

Theorem on polynomial approximation

Let f be an analytic function in $[-1,1]$ which is bounded by 1 in a complex ellipse E_ρ around $[-1,1]$. Then for $\delta \ll (\rho-1)^2$, and parameters $\varepsilon \in (0,1)$, and $b > 1$, there is a polynomial q of degree $O(\frac{b}{\delta}\log\frac{b}{\delta\varepsilon})$ with the form:



Thank you!

For further reading:

- Paige and Wei, *History and generality of the CS decomposition*
- Edelman and Jeong, *Fifty three matrix factorizations: A systematic approach*
- Trefethen, *Approximation theory and approximation practice*
- Martyn, Rossi, Tan, and Chuang, *A grand unification of quantum algorithms*