Advanced quantum algorithms for scientific computing

Agnieszka Międlar and Paul Cazeaux

Department of Mathematics, Virginia Tech
amiedlar@vt.edu and pcazeaux@vt.edu

CEMRACS Summer School 2025 on Quantum Computing
CIRM, July 15-19, 2025

Outline

Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy.

Richard Feynman, 1981 lecture on *Simulating physics with computers.*

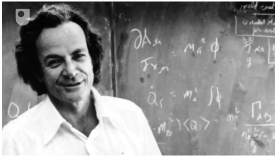


Figure 1: Credit: Britannica.

This talk is based on:

Di Fang (2024) *MATH 690: Quantum Scientific Computing*, Lecture Notes.

Lin Lin (2023) *Lecture Notes on Quantum Algorithms for Scientific Computation*.

Camps et al. (2022) *FABLE: Fast Approximate Quantum Circuits for Block-Encoding*.

Kirby et al. (2023) *Exact and Efficient Lanczos Method on a Quantum Computer*.

Deep Learning University (2025) *Quantum Computing Tutorials*.

IBM Quantum Platform (2025) *Quantum Learning*.

Dong An (2023) *Introduction to Quantum Numerical Linear Algebra*.

De Wolf (2019) *Quantum Computing: Lecture Notes*.

Nielsen and Chuang (2001) *Quantum Computation and Quantum Information*.

Childs (2022) *Lecture Notes on Quantum Algorithms*.

Preskill (1998) *Lecture Notes for Physics 229: Quantum Information and Computation*.

Other See Bibliography at the end.

Prerequisites

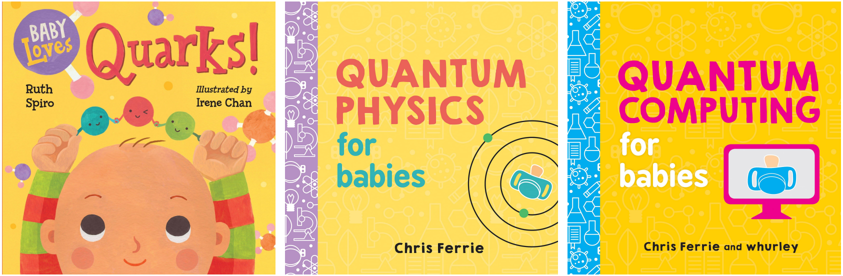


Figure 2: Credit: Amazon

If you have questions, please ask Lucie offline!

A Bit of Early History in Nutshell

Manin, Feymann and Benioff (early 1980s) on analog quantum computer and computational power beyond that of traditional computations.

Deutsch (1985) the universal quantum Turing machine.

Figure 3: Credit: Wikipedia.

Deutsch and Jozsa (1992) one of the first quantum algorithm that is exponentially faster than any possible deterministic classical algorithm, i.e., given an oracle that implements $f : \{0,1\}^n \rightarrow \{0,1\}$ determine if f is constant or balanced.

Bernstein and Vazirani (1993) quantum complexity theory.

Simon (1994) a polynomial-time algorithm for a quantum computer that distinguishes between two classes of polynomial-time computable function, i.e., exponential quantum speedup for finding the period of a 2 to 1 function.

Shor (1994) efficient quantum algorithms for the problems of integer factorization and discrete logarithms.

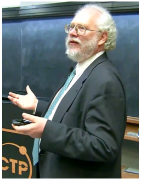


Figure 4: Credit: Wikipedia.

Google (2019) "quantum supremacy" experiment on 53 qubits.

Figure 5: Credit: Google.

The Four Main Postulates of Quantum Mechanics

1. State Space Postulate

- A **quantum state** $|\psi\rangle \in \mathcal{H}$ is a superposition of classical states, written as a vector of amplitudes, to which we can apply either a measurement or a unitary operation.

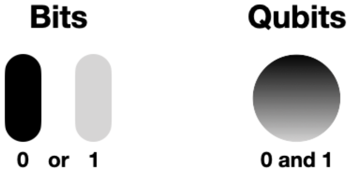


Figure 6: Credit: Deep Learning University, Qiskit Tutorial, 2025

- We use **Dirac notation**, i.e.,

  $|\cdot\rangle$ **ket:** a column vector $|\psi\rangle = \begin{bmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{N-1} \end{bmatrix}$,

  $\langle\cdot|$ **bra:** a row vector, Hermitian conjugation of a quantum state $|\psi\rangle \in \mathcal{H}$

$$\langle\psi| = |\psi\rangle^* = \begin{bmatrix} \overline{\psi}_0 & \overline{\psi}_1 & \dots & \overline{\psi}_{N-1} \end{bmatrix},$$

  $\langle\cdot|\cdot\rangle$ **braket:** inner product $\langle\psi|\phi\rangle$

$$\langle\psi|\phi\rangle = (\psi, \phi) \in \mathbb{C}.$$

- We will always assume that $|\psi\rangle$ is normalized, i.e., $\langle\psi|\psi\rangle = 1$. Hence, $\mathcal{H} \cong \mathbb{C}^N / \|\cdot\|_2$.

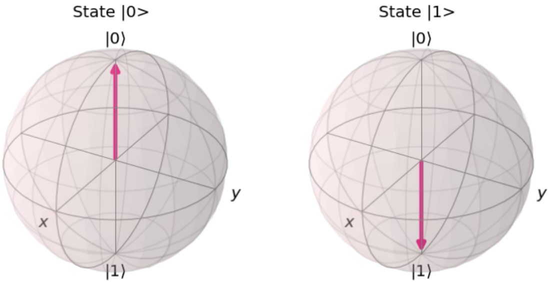
- The set of all quantum states of a quantum system forms a complex vector space with inner product (Hilbert space denoted as $\mathcal{H}$), called the **state space**.
- If $\mathcal{H}$ is finite dimensional it is isomorphic to some $\mathbb{C}^N$.
- W.l.o.g we can take $\mathcal{H} = \mathbb{C}^N$, where $N = 2^n$, $n \in \mathbb{Z}_+$ is called the number of **quantum bits** (**qubits**).

Figure 7: Credit: Deep Learning University, Qiskit Tutorial, 2025

Example (Single Qubit System)

$\mathcal{H} \cong \mathbb{C}^N / \|\cdot\|_2$

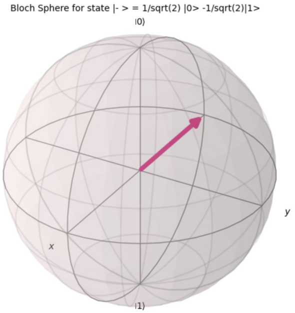
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{(spin-up)}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{(spin-down)}$$




```
plot_bloch_vector([0, 0, 1], title="Bloch Sphere for state |0>")
plot_bloch_vector([0, 0, -1], title="Bloch Sphere for state |1>")
```

Probabilities on Measurements

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \in \mathcal{H}.$$




```
plot_bloch_vector([-1, 0, 0], ...
        title="Bloch Sphere for state |- > = 1/sqrt(2)|0> - 1/sqrt(2)|1>")
```

Normalization condition implies $|a|^2 + |b|^2 = 1$.
If we perform a measurement we will get $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ with probability $|b|^2$.

Example

Let us calculate the probabilities of measuring 0 and 1 upon measurement of a qubit in the state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. The probability of obtaining 0 on measurement is given as

$$p(0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

Similarly, the probability of obtaining 1 on measurement can be calculated as

$$p(1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}.$$

Since both coefficients for $|0\rangle$ and $|1\rangle$ are equal, the probabilities of obtaining 0 and 1 on measurement are the same. Also the resulting probabilities of measuring 0 and 1 add up to 1, as they should.

- $|x, y\rangle$ represents **Kronecker product** of $|x\rangle$ and $|y\rangle$, which can also be written as $|x\rangle\,|y\rangle$ or $|xy\rangle$.
- Kronecker product of m $|0\rangle$'s is denoted by $|0^m\rangle$ or $|0\rangle^{\otimes m}$.
- $\mathbf{I}_N$ denotes the $N \times N$ **identity matrix**.
- The j^{th} column of matrix $\mathbf{I}_N$ is denoted by $|j\rangle$ for $j = 0, 1, \ldots, N-1$.
- The **binary representation of** $j \in \mathbb{N}, 0 \leq j \leq 2^n - 1$ is given by

$$j = [j_{n-1} \ldots j_1\ j_0] = j_{n-1} \cdot 2^{n-1} + \ldots + j_1 \cdot 2^1 + j_0 \cdot 2^0.$$

2. Quantum Operator Postulate

- The evolution of a quantum state from $|\psi\rangle$ to $|\psi'\rangle$ is always achieved via a unitary operator $\mathbf{U} \in \mathbb{C}^N \times \mathbb{C}^N$, i.e.,

$$\left|\psi'\right\rangle = \mathbf{U}\left|\psi\right\rangle, \quad \mathbf{U}^*\mathbf{U} = \mathbf{I}_N.$$

- In quantum computation, a unitary matrix (operator) is referred as a **gate**.
- An operator acting on an n-qubit quantum state space $\mathcal{H}$ is called ***n*-qubit operator**.

Example (Single Qubit Operators)

Hadamard $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Pauli matrices

$$\sigma_x = \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \mathbf{Y} = \begin{bmatrix} 0 & -\imath \\ -\imath & 0 \end{bmatrix}, \quad \sigma_z = \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Rotation along Pauli-Y axis $\mathbf{R}_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = e^{-\imath\theta Y/2}$

Phase $\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}$

Two-Qubit Operators

controlled not (CNOT) $\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

SWAP $\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

3. Quantum Measurement Postulate (Projective Measurement)

- If we measure quantum state $|\psi\rangle$, we **cannot "see" superposition**. We only can get a **classical state $|j\rangle$**, $\quad j = 0, \ldots, N-1$.

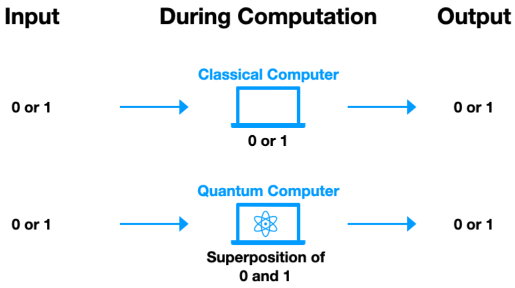


Figure 8: Credit: Deep Learning University, Qiskit Tutorial, 2025

- We do not know in advance which $|j\rangle$ we get, we only know the probability $|\alpha_j|^2$ of observing $|j\rangle$ (**Born's rule)**.

- If we measure $|\psi\rangle$ and get $j = 0$, then state $|\psi\rangle$ disappears, and all that is left is $|j\rangle$, i.e., **observing the state $|\psi\rangle$ "collapses" it to the classical state $|j\rangle$**.
- Quantum observables (in finite dimension) always correspond to a Hermitian matrix with spectral decomposition

$$M = \sum_m \lambda_m P_m, \quad \text{with} \quad \lambda_m \in \mathbb{R} \quad \text{and} \quad P_m^2 = P_m.$$

- The outcome of a **measurement of a quantum state $|\psi\rangle$ by a quantum observable M is an eigenvalue λ_m** with probability $p_m = \langle\psi| P_m |\psi\rangle$. After the measurement

$$|\psi\rangle \to \frac{P_m |\psi\rangle}{\sqrt{p_m}}.$$

  However, this is not a unitary process.
- The expectation value of the measurement outcome is

$$\mathbb{E}_\psi(M) = \langle\psi| M |\psi\rangle .$$

4. Tensor Product Postulate

- An element (quantum state) in the ***n*-qubit state space** $\mathcal{H} = (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ can be written as

$$|\psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle,$$

where single qubit states $|j\rangle, 0 \leq j \leq 2^n - 1$ are orthonormal basis of $\mathcal{H}$. A complex number α_j is called the amplitude of $|j\rangle$ in $|\psi\rangle$.

- If $\psi \in \mathbb{C}^{2^n}$, we can use the following notation

$$\begin{aligned} |\psi\rangle &= |\psi_0\rangle \otimes |\psi_1\rangle \otimes \ldots \otimes |\psi_{m-1}\rangle \\ &\equiv |\psi_0\psi_1 \ldots \psi_{m-1}\rangle \equiv |\psi_0, \psi_1, \cdots, \psi_{m-1}\rangle \\ &\equiv |\psi_0\rangle |\psi_1\rangle \ldots |\psi_{m-1}\rangle. \end{aligned} \tag{1}$$

- $\psi \in \{0,1\}^n$ is called a **classical bit-string** and $|\psi\rangle, \psi \in \{0,1\}^n$ **the computational basis** of $\mathbb{C}^{2^n}$.

Example (Two Qubit System)

The state space of two qubit system is $\mathcal{H} = (\mathbb{C}^2)^{\otimes 2} \cong \mathbb{C}^4$ with standard basis

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

If a quantum state $|\psi\rangle$ has m components with state spaces $\{\mathcal{H}_i\}_{i=0}^{m-1}$, its state space is a tensor product denoted by $\mathcal{H} = \otimes_{i=0}^{m-1}\mathcal{H}_i$ and

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \cdots \otimes |\psi_{m-1}\rangle, \quad \text{where } |\psi_i\rangle \in \mathcal{H}_i.$$

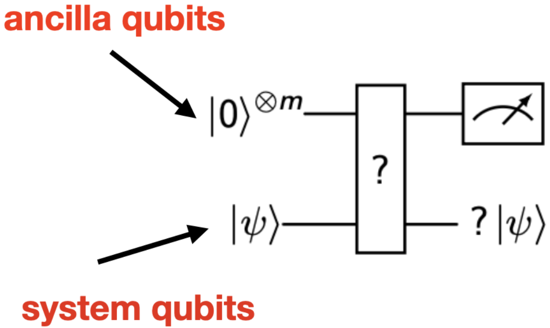
However, not all quantum states in $\mathcal{H}$ can be written in this form, e.g., the Bell state (the EPR pair)

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}.$$

Quantum Circuits

System registers (*signal qubits*): storing quantum states of interest.

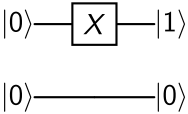
Ancilla registers (*ancilla qubits*): auxiliary registers needed to implement the unitary operation acting on system registers.



Example Quantum Circuits

Pauli X gate

$$X|0\rangle = |1\rangle$$

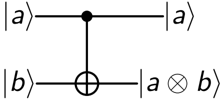


$$(X \otimes I)|00\rangle = |10\rangle$$

Hadamard gate

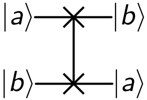
$$H\left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right) = \begin{bmatrix} 0.986 \\ -0.169 \end{bmatrix}$$

CNOT gate



$$CNOT|00\rangle = |10\rangle$$

SWAP gate



$$SWAP|10\rangle = |01\rangle$$

Outline

QuantNLA: Expectations and Restrictions

- Quantum computers are known to provide **exponential quantum speedups** for some problems, so it is natural to understand what they can do in linear algebra problems.
- Typical cost of **classical algorithm for N-dimensional system is** $poly(N)$ **vs. expected** $\mathcal{O}(poly\ log(N))$ **cost for quantum algorithms**.

No-cloning Theorem (Wootters & Zurek, Dieks 1982)

Consider two quantum systems S_1 and S_2 with a common Hilbert space $\mathcal{H} = \mathcal{H}_{S_1} = \mathcal{H}_{S_2}$. There is no unitary operator $\mathbf{U}$ on $\mathcal{H} \otimes \mathcal{H}$ such that for all normalized states $|\psi\rangle_{S_1}$ and $|e\rangle_{S_2}$ in $\mathcal{H}$

$$\mathbf{U}\left(|\psi\rangle_{S_1} |e\rangle_{S_2} \right) = e^{\imath\alpha} |\psi\rangle_{S_1} |\psi\rangle_{S_2} ,$$

where α depends on $|\psi\rangle$ and $|e\rangle$.

- **forbids** generic **quantum copy operation**,
- all **classical iterative algorithms are not feasible** for quantum computing as they require storing intermediate information.

Two exceptions of the No-cloning Theorem

- If we know how a quantum state is prepared, i.e., $|\psi\rangle = \mathbf{U}_\psi |\phi\rangle$ for a known unitary $\mathbf{U}_\psi$ and some $|\phi\rangle$, then we can copy $|\psi\rangle$ via

$$(\mathbf{I} \otimes \mathbf{U}_\psi) |\psi\rangle \otimes |\phi\rangle = |\psi\rangle \otimes |\psi\rangle .$$

- **CNOT** gate **enables copying classical information**, i.e.,

$$CNOT |\psi, 0\rangle = |\psi, \psi\rangle , \quad \psi \in \{0, 1\}.$$

  However, it can not be used to copy a superposition of classical bits $|\psi\rangle = a|0\rangle + b|1\rangle$, i.e.,

$$CNOT |\psi\rangle \otimes |0\rangle = a|00\rangle + b|11\rangle \neq |\psi\rangle \otimes |\psi\rangle .$$

No-deleting Theorem

There is **no unitary operator U** such that

$$\mathbf{U} |0^n\rangle \otimes |x\rangle = |0^n\rangle \otimes |0^n\rangle .$$

- given two copies of a quantum state it is impossible to remove one copy (consequence of No-cloning Theorem).

The Problem of the Input Model

How to get information in a vector $v \in \mathbb{C}^N$ or a matrix $A \in \mathbb{C}^{N\times N}$ into the quantum computer?

Input Model for Vectors in $\mathbb{C}^N$

- The n-qubit **quantum state** $|\psi\rangle$ can be viewed as $N = 2^n$-dimensional vector normalized under 2-norm (some information may be lost).
- The cost of storing n-qubit quantum state is $\sim N$.

Black-box quantum state preparation (state preparation oracle)

Goal: Construct an n-qubit state $|\psi\rangle$ given as a (quantum) oracle

$$\mathbf{U}_\psi : |0\rangle \to |\psi\rangle = \sum_{j=0}^{2^n-1} \psi_j |j\rangle .$$

- Amplitudes ψ_j are unknown a priori and can only be accessed through an oracle or black-box.
- Each amplitude ψ_j is encoded with n-bit precision.
- The oracle $\mathbf{U}_\psi$ can be invoked, as required, with complexity $\mathcal{O}(1)$.

Quantum State Preparation Algorithms

Grover and Rudolph (2002) given a certain probability distribution $\{p_j\}$, how to efficiently create a quantum superposition $|\psi\rangle = \sum_j p_j |j\rangle$.

Sun et al. (2021) asymptotically optimal circuit depth for quantum state preparation, $\Theta(2^n/n)$ (no ancillary qubits), $\Theta(n)$ (with $\mathcal{O}(2^n)$ ancillary qubits).

Araujo et al. (2021) asymptotically optimal circuit depth for quantum state preparation $\Theta(n)$ (with $\widetilde{\mathcal{O}}(2^n)$ ancillary qubits).

Rosenthal (2022) asymptotically optimal circuit depth for quantum state preparation $\Theta(n)$ (with $\widetilde{\mathcal{O}}(2^n)$ ancillary qubits).

Zhang, Li and Yuan (2023) any n-qubit quantum state can be prepared with a $\Theta(n)$-depth circuit using only single- and two-qubit gates (with $\mathcal{O}(2^n)$ ancillary qubits). For sparse quantum states with $d > 2$ nonzero entries, circuit depth to $\Theta(log(nd))$ with $\mathcal{O}(nd\ log(d))$ ancillary qubits.

Laneve (2023) quantum state preparation using quantum signal processing (QSP) and quantum singular value transform (QSVT) within error ε in time $\mathcal{O}(\sqrt{\gamma}T(n)log(1/\varepsilon))$ and $\lceil 2 + log_2(6/\varepsilon\gamma) \rceil$ additional qubits, where $\mathcal{O}(T(n))$ is time for amplitude computations and $\sqrt{\gamma}$ is an inverse polynomial in n.

Block-Encoding (BE) = Input Model for Matrices

Step 1: embed a (non-unitary) matrix $\mathbf{A}$, $\|\mathbf{A}\|_2 \leq \alpha$ into a unitary matrix $\mathbf{U}_A$ of larger size (after appropriate scaling), i.e.,

$$\mathbf{U}_A = \begin{bmatrix} \frac{1}{\alpha}\mathbf{A} & * \\ * & * \end{bmatrix},$$

Step 2: convert unitary $\mathbf{U}_A$ into a quantum circuit (express $\mathbf{U}_A$ as a product of simpler unitaries) to allow computation on quantum computer.

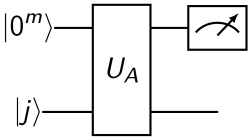


Figure 9: Circuit for General Block-encoding of A.

Such an encoding is useful if $\mathbf{U}_A$ can be implemented efficiently.

Definition 1 (**Block-encoding (BE) [Chakraborty et al., 2019, Camps et al., 2024]**)

Given an n-qubit matrix $\mathbf{A}$ ($\mathbf{A}$ is of size $N \times N$ with $N = 2^n$), if we can find $\alpha, \varepsilon \in \mathbb{R}_+$, and an $(m+n)$-qubit unitary matrix $\mathbf{U}_A$ ($\mathbf{U}_A$ is of size $2^{n+m} \times 2^{n+m}$) such that

$$\|\mathbf{A} - \alpha\big(\langle 0|^{\otimes m} \otimes I_n\big) U_A \big(|0\rangle^{\otimes m} \otimes I_n\big)\|_2 \le \varepsilon,$$

then $\mathbf{U}_A$ is called an (α, m, ε)-block-encoding of $\mathbf{A}$. If the block-encoding is exact with $\varepsilon = 0$, $\mathbf{U}_A$ is called an (α, m)-block-encoding of $\mathbf{A}$.

Here α is the block-encoding factor (subnormalization factor) that satisfies $\alpha \ge \|\mathbf{A}\|$ and m is the number of ancilla qubits used to block encode $\mathbf{A}$.

Simple check using matrix form:

Since $\langle 0^m| \otimes \mathbf{I}_n = \begin{bmatrix} \mathbf{I}_n & 0 \end{bmatrix}$ and $|0^m\rangle \otimes \mathbf{I}_n = \begin{bmatrix} \mathbf{I}_n \\ 0 \end{bmatrix}$, then

$$\alpha\big(\langle 0|^{\otimes m} \otimes \mathbf{I}_n\big)\mathbf{U}_A\big(|0\rangle^{\otimes m} \otimes I_n\big) = \alpha \begin{bmatrix} \mathbf{I}_n & 0 \end{bmatrix} \begin{bmatrix} \frac{\mathbf{A}}{\alpha} & * \\ * & * \end{bmatrix} \begin{bmatrix} \mathbf{I}_n \\ 0 \end{bmatrix} = \mathbf{A}.$$

Block-Encoding: Existence and Uniqueness

Theorem 2 (**Existence of BE [Alber et al., 2003]**)

Every non-unitary matrix $\mathbf{A}$ *can be embeded in a* $(\|\mathbf{A}\|_2, 1)$*-block-encoding.*

Proof: W.lo.g. assume that $\|\mathbf{A}\| \leq 1$ (otherwise consider $\frac{A}{\alpha}$). Consider Singular Value Decomposition (SVD) of matrix $\mathbf{A}$, i.e., $\mathbf{A} = \mathbf{W} \circ \mathbf{V}^*$ (all $\sigma_j \in [0, 1]$). Then

$$\mathbf{U}_A = \begin{bmatrix} \mathbf{W} & \\ & \mathbf{I}_n \end{bmatrix} \begin{bmatrix} \Sigma & \sqrt{\mathbf{I}_n - \circ^2} \\ \sqrt{\mathbf{I}_n - \circ^2} & -\circ \end{bmatrix} \begin{bmatrix} \mathbf{V}^* & \\ & \mathbf{I}_n \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{A} & \mathbf{W}\sqrt{\mathbf{I}_n - \circ^2} \\ \sqrt{\mathbf{I}_n - \circ^2}\,\mathbf{V}^* & -\circ \end{bmatrix}.$$

Some Simple Block-Encodings

"tivial" example Let **U** be a unitary matrix, then **U** is a $(1, 0, 0)$-block-encoding of itself.

a scalar $0 < \alpha < 1$ Let $\mathbf{A} = \alpha \in \mathbb{C}^{1\times 1}$. Then a block-encoding of **A** can be constructed as

$$\mathbf{U}_A = \begin{bmatrix} \alpha & \sqrt{1-\alpha^2} \\ \sqrt{1-\alpha^2} & -\alpha \end{bmatrix} \quad \text{or} \quad \mathbf{U}_A = \begin{bmatrix} \alpha & -\sqrt{1-\alpha^2} \\ \sqrt{1-\alpha^2} & \alpha \end{bmatrix}.$$

Remark 3

This answers the uniqueness question.

$\|\mathbf{A}\|_2 \leq \mathbf{1}$ Then a block-encoding of $\mathbf{A}$ can be constructed as

$$\mathbf{U}_A = \begin{bmatrix} \mathbf{A} & \sqrt{\mathbf{I} - \mathbf{A}^*\mathbf{A}} \\ \sqrt{\mathbf{I} - \mathbf{A}^*\mathbf{A}} & -\mathbf{A} \end{bmatrix} \text{ or } \mathbf{U}_A = \begin{bmatrix} \mathbf{A} & \sqrt{\mathbf{I} - \mathbf{A}^*\mathbf{A}} \\ \sqrt{\mathbf{I} - \mathbf{A}^*\mathbf{A}} & \mathbf{A} \end{bmatrix} \quad (2)$$

Existence is not all

This block-encoding requires computing the square root of $\mathbf{A}^*\mathbf{A}$ which cannot be done efficiently on quantum computer using $\mathcal{O}(poly(n))$ quantum gates. Theorem 2 does not guarantee the existence of an efficient quantum circuit implementation.

Some Good News [Camps et al., 2024]

2×2 **symmetric matrix** Let us consider $\mathbf{A} = \frac{1}{2}\begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix}$, with $0 \leq |\alpha_1|, |\alpha_2| \leq 1$. Then a block-encoding of $\mathbf{A}$ can be constructed as

$$\mathbf{U_A} = \frac{1}{2}\begin{bmatrix} \mathbf{U}_\alpha & -\mathbf{U}_\beta \\ \mathbf{U}_\beta & \mathbf{U}_\alpha \end{bmatrix},$$

where

$$\mathbf{U}_\alpha = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_1 & -\alpha_2 \\ \alpha_2 & \alpha_1 & -\alpha_2 & \alpha_1 \\ \alpha_1 & -\alpha_2 & \alpha_1 & \alpha_2 \\ -\alpha_2 & \alpha_1 & \alpha_2 & \alpha_1 \end{bmatrix} \quad \text{and} \quad \mathbf{U}_\beta = \begin{bmatrix} \beta_1 & \beta_2 & \beta_1 & -\beta_2 \\ \beta_2 & \beta_1 & -\beta_2 & \beta_1 \\ \beta_1 & -\beta_2 & \beta_1 & \beta_2 \\ -\beta_2 & \beta_1 & \beta_2 & \beta_1 \end{bmatrix},$$

with $\beta_1 = \sqrt{1 - \alpha_1^2}$ and $\beta_2 = \sqrt{1 - \alpha_2^2}$.

Define $\phi_1 = \arccos(\alpha_1) + \arccos(\alpha_2)$ and $\phi_2 = \arccos(\alpha_1) - \arccos(\alpha_2)$, then the block encoding U_A can be factored as a product of simpler unitaries, i.e.,

$$\mathbf{U}_A = \mathbf{U_6 U_5 U_4 U_3 U_2 U_1 U_0},$$

where

- $U_0 = U_6 = I_2 \otimes H \otimes I_2$,
- $U_1 = R_1 \otimes I_2 \otimes I_2$,
- $U_2 = U_4 = (I_2 \otimes E_0 + X \otimes E_1) \otimes I_2$,
- $U_3 = R_2 \otimes I_2 \otimes I_2$,
- $U_5 = I_2 \otimes (E_0 \otimes I_2 + E_1 \otimes X)$,

with

$\mathbf{H}, \mathbf{X}$	the Hadamard and Pauli- X gates, respectively,
$\mathbf{R}_1, \mathbf{R}_2$	rotation matrices $R_1 = R_y(\phi_1)$, $R_2 = R_y(\phi_2)$, and
$\mathbf{E}_0, \mathbf{E}_1$	projectors, i.e., $E_0 = e_0 e_0^T = \|0\rangle \langle 0\|$, $E_1 = e_1 e_1^T = \|1\rangle \langle 1\|$.

The quantum circuit associated with the factorization is given as

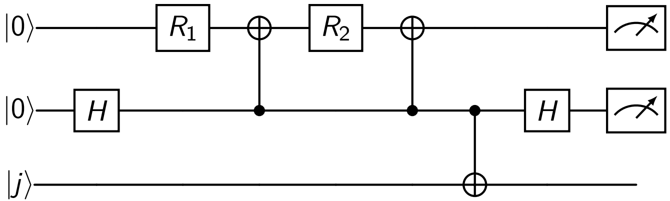


Figure 10: Circuit for General Block-encoding of a 2×2 symmetric matrix A.

Remark 4

Note that the unitary that block encodes the 2×2 *matrix* $\mathbf{A}$ *is of dimension* 2^3*, i.e.,* 2 *ancilla qubits in addition to the* $n = 1$ *system qubit required to match the dimension of* $\mathbf{A}$*, which is* $N = 2^n$*. It is twice the dimension of the block encoding given through* (2) *(one using square root of* $\mathbf{A}^*\mathbf{A}$*).*

Some Good News = Block-Encoding in Practice

Block-encoding of a general matrix is hard, however, there are some success stories:

sparse matrices: based on "query oracles" giving the position and binary description of matrix entries [Berry et al., 2015b, Gilyén et al., 2019, Childs et al., 2017], specific $2^n \times 2^n$ in $poly(n)$ complexity [Camps et al., 2024],

quantum walks on highly-structured graphs: [Szegedy, 2004, Childs, 2010, Loke and Wang, 2017],

structured matrices: [Sünderhauf et al., 2024],

dense and full-rank kernels: using hierarchical matrices [Nguyen et al., 2022],

pseudo-differential operators: efficient and explicit BE algorithm [Li et al., 2023],

pairing Hamiltonian: [Liu et al., 2025].

...

State-of-the-art for sparse A

Assume that $\mathbf{A}$ is a s-sparse matrix with $\|\mathbf{A}\| \leq 1$.

- encode the position and the numerical value of the nonzero matrix elements through the following oracles, i.e.,

$$
\begin{aligned}
\mathbf{O}_{\text{row}} |j, nz\rangle &= |j, \text{row}(j, nz)\rangle \\
\mathbf{O}_{\text{col}} |j, nz\rangle &= |j, \text{col}(j, nz)\rangle \\
\mathbf{O}_{A}|j, k, z\rangle &= |j, k, z \oplus A_{jk}(t)\rangle ,
\end{aligned}
$$

  where $\text{row}(j, nz)$ is the row index of the nz^{th} nonzero element in the j^{th} column, $\text{col}(j, nz)$ is the column index of the nz^{th} nonzero element in the j^{th}row, with $j \in 1, \ldots, N$ and $nz \in 1, \ldots, s$ [Berry and Childs, 2009, Childs et al., 2017].

- combine these query oracles into **matrix query oracle** [Lin, 2022] to enable access to the matrix data.

A $(s, n+3, \varepsilon)$-**block-encoding** of $\mathbf{A}$ can be constructed via $\mathcal{O}(1)$ **queries** to above oracles and $\mathcal{O}\left(n + \log^{5/2}(s/\varepsilon)\right)$ **primitive gates**.

Fast Approximate BLock-Encodings (FABLE) [Camps and Van Beeumen, 2022]

- **F**ast **A**pproximate **BL**ock-**E**ncodings (**FABLE**) [Camps and Van Beeumen, 2020, Camps and Van Beeumen, 2022] generates quantum circuits that block encode **arbitrary matrices up to prescribed accuracy**,
- defines a matrix query operation $\mathbf{O}_A$ for a given matrix $\mathbf{A}$ which is then synthesized in a quantum circuit.

Definition 5 (**Matrix Query Operation $\mathbf{O}_A$**)

Let $A = [a_{ij}], i, j = 1, \ldots, N$, with $N = 2^n$ and $\|a_{ij}\| \leq 1$. Then the matrix query operation $\mathbf{O}_A$ applies

$$\mathbf{O}_A \left|0\right\rangle \left|i\right\rangle \left|j\right\rangle = \left(a_{ij} \left|0\right\rangle + \sqrt{1 - |a_{ij}|^2} \left|1\right\rangle\right) \left|i\right\rangle \left|j\right\rangle,$$

where $\left|i\right\rangle$ and $\left|j\right\rangle$ are n-qubit computational basis states.

High-level Quantum Circuit

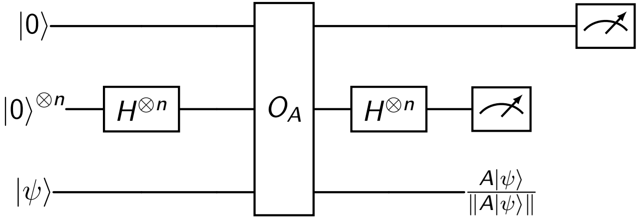


Figure 11: High-level quantum circuit structure for FABLE block-encoding a matrix $\mathbf{A}$ in terms of a matrix query oracle $\mathbf{O}_A$.

- all information about the matrix are encoded in a **single matrix query oracle** which can be implemented with simple one-qubit $\mathbf{R}_y$ and $\mathbf{R}_z$ rotations, two-qubit **CNOT** gates, and some additional **Hadamard** and **SWAP** gates
- the gate **complexity of a FABLE circuit** for general, unstructured $N \times N$ matrix is bounded by $\mathcal{O}(N^2)$ (with prefactor 2 for real and 4 for complex matrices) plus limited polylogarithmic overhead.

Let us verify that the circuit $\mathbf{U}_A$ in Figure (11) is indeed an $(1/2^n, n+1)$ encoding of an n-qubit matrix $\mathbf{A}$, i.e., satisfies Definition 1.

The circuit $\mathbf{U}_A$ can be written in matrix notation as

$$\mathbf{U}_A = (I_1 \otimes H^{\otimes n} \otimes I_n)(I_1 \otimes SWAP)O_A(I_1 \otimes H^{\otimes n} I_n).$$

For U_A to satisfy Definition 1 we need

$$\langle 0| \left\langle 0\right|^{\otimes n} \langle i|U_A \mid 0\rangle \left|0\right\rangle^{\otimes n}|j\rangle = \frac{1}{2^n} a_{ij}.$$

First, we have

$$\begin{aligned}
|0\rangle|0\rangle^{\otimes n}|j\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |0\rangle|k\rangle|j\rangle, \\
&\xrightarrow{O_A} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left(a_{kj}|0\rangle + \sqrt{1-|a_{kj}|^2}|1\rangle \right) |k\rangle|j\rangle, \\
&\xrightarrow{\text{SWAP}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left(a_{kj}|0\rangle + \sqrt{1-|a_{kj}|^2}|1\rangle \right) |j\rangle|k\rangle.
\end{aligned}$$

Similarily,

$$|0\rangle|0\rangle^{\otimes n}|i\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{\ell=0}^{2^n-1} |0\rangle|\ell\rangle|i\rangle.$$

Now combining both, yields

$$\begin{aligned}
&\langle 0| \left\langle 0\right|^{\otimes n} \langle i| U_A |0\rangle|0\rangle^{\otimes n}|j\rangle \\
&\quad = \frac{1}{2^n} \left(\sum_{\ell=0}^{2^n-1} \langle 0|\langle \ell|\langle i| \right) \\
&\qquad \left(\sum_{k=0}^{2^n-1} \left(a_{kj}|0\rangle + \sqrt{1-|a_{kj}|^2}|1\rangle \right) |j\rangle|k\rangle \right), \\
&\quad = \frac{1}{2^n} \sum_{\ell=0}^{2^n-1} \sum_{k=0}^{2^n-1} a_{kj} \langle \ell \mid j\rangle\langle i \mid k\rangle \\
&\quad = \frac{1}{2^n} a_{ij}.
\end{aligned}$$

which completes the proof.

$\mathbf{A} \in \mathbb{R}^{N\times N}$ For given row and column indices i and j, $\mathbf{O}_A$ acts on the $|0\rangle$ state of the first qubit as an $\mathbf{R}_y$ gate with angle $\theta_{ij} = \arccos(a_{ij})$, i.e.,

$$\mathbf{R}_y(2\theta_{ij})|0\rangle = \begin{bmatrix} \cos(\theta_{ij}) & -\sin(\theta_{ij}) \\ \sin(\theta_{ij}) & \cos(\theta_{ij}) \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a_{ij} \\ \sqrt{1-a_{ij}^2} \end{bmatrix}$$

Hence, the matrix query unitary $\mathbf{O}_A$ for a real-valued matrix is a matrix with the following structure

$$\mathbf{O}_A = \begin{bmatrix} c_{00} & & & & & -s_{00} & & \\ & c_{01} & & & & & & \\ & & \ddots & & & & & \\ & & & c_{N-1,N-1} & & & & \\ s_{00} & & & & c_{00} & & & -s_{N-1,N-1} \\ & s_{01} & & & & c_{01} & & \\ & & \ddots & & & & \ddots & \\ & & & s_{N-1,N-1} & & & & c_{N-1,N-1} \end{bmatrix},$$

where $c_{ij} := \cos(\theta_{ij})$ and $s_{ij} := \sin(\theta_{ij})$.

For details see

[Camps and Van Beeumen, 2020, Camps and Van Beeumen, 2022].

Block encoding = Standard-Form Encoding

Definition 6 (**Standard-form Encoding [Low and Chuang, 2019]**)

A signal operator $\mathbf{H}$ (acting on a Hilbert space $\mathcal{H}_s$ whose states are denoted $|\cdot\rangle_s$) with spectral norm $\|\mathbf{H}\| \leq 1$ is encoded in the standard-form if we may query a unitary oracle $\mathbf{U} : \mathcal{H}_a \otimes \mathcal{H}_s \to \mathcal{H}_a \otimes \mathcal{H}_s$ (for some auxiliary Hilbert space $\mathcal{H}_a$ whose states are denoted $|\cdot\rangle_a$) and a unitary state preparation oracle $|G\rangle_a := G|0\rangle_a \in \mathcal{H}_a$ such that

$$(\langle G|_a \otimes \mathbf{I}_s)\, \mathbf{U}\, (|G\rangle_a \otimes \mathbf{I}_s) = \mathbf{A}\ . \tag{3}$$

A pair $(\mathbf{U}, \mathbf{G})$ is called a **standard-form encoding** of $\mathbf{A}$. Here $\mathbf{I}_s$ denotes identity acting on $\mathcal{H}_s$.

Remark 7

Note that choosing $|G\rangle_a := G|0\rangle_a = |0\rangle^{\otimes m}$ immediately provides equivalence with Definition 1.

Matrix-vector Product

Input: n-qubit quantum matrix $\mathbf{A}$ and quantum state $|\psi\rangle$

Step 1 Block-encode $\mathbf{A}$, $\|\mathbf{A}\| \leq 1$, i.e.,

$$\mathbf{U}_A = \begin{bmatrix} \frac{1}{\alpha}\mathbf{A} & * \\ * & * \end{bmatrix}.$$

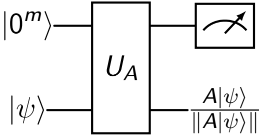
Step 2 Apply $\mathbf{U}_A$ to an "extended" vector $|0^m, \psi\rangle = \underbrace{|0^m\rangle}_{\text{ancilla}} \underbrace{|\psi\rangle}_{\text{system}} = \begin{bmatrix} \psi \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, i.e.,

$$\mathbf{U}_A |0^m, \psi\rangle = \begin{bmatrix} \frac{1}{\alpha}\mathbf{A} & * \\ * & * \end{bmatrix} \begin{bmatrix} \psi \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} \mathbf{A}\psi \\ * \end{bmatrix} = \begin{bmatrix} \mathbf{A}\psi \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ * \end{bmatrix} = |0\rangle |\mathbf{A}\psi\rangle + \underbrace{|1\rangle |*\rangle}_{\text{unnormalized state}} .$$

Step 3 "Get" the product $A|\psi\rangle$ by measuring the ancilla qubits

$$(|0\rangle\langle 0| \otimes I)(|0\rangle |A\psi\rangle + |1\rangle |*\rangle) = |0\rangle |A\psi\rangle .$$

Circuit for Matrix-vector Product



- To obtain $\mathbf{A}\,|\psi\rangle$, we need to **measure the qubit** 0 and only keep the state if it returns 0.
- Provided the outcome of the measurement on the first wire is $|0^m\rangle$ then the output of the circuit is $(\|A\,|\psi\rangle\,\|/\alpha)^2$.
- Need to **measure the first ancilla qubit**.
- The **success probability** of this measurement is $(\|A\,|\psi\rangle\,\|/\alpha)^2$.

Quantum vs Classical Numerical Linear Algebra

	Classical	Quantum
State space	$N = 2^n$	n
Space elements	N-dimensional vectors	n-qubit quantum state (N-dimensional unit vector)
Cost	$\mathcal{O}(poly(N))$	$\mathcal{O}(poly\ log(N)) = \mathcal{O}(poly(n))$
Vectors (entries)	☺	☹
Matrices	any	unitary
Copying information	☺	☹

Outline

The Quantum Fourier Transform (QFT)

Let $\omega_N = e^{2\pi\imath/N}$ be an N-th root of unity, i.e., $\omega_N^N = 1$. Then an $N \times N$ unitary matrix

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} & \vdots & \\ \cdots & \omega_N^{jk} & \cdots \\ & \vdots & \end{bmatrix}$$

is called the **Fourier transform**.

- Since F_N is unitary and symmetric, $F_N^{-1} = F_N^*$.
- The naive way of computing the Fourier transform of $\widehat{v} = F_N v$ of vector $v \in \mathbb{R}^N$ would take $\mathcal{O}(N^2)$ steps.
- A more practical way is through the **Fast Fourier Transform** [Cooley and Tukey, 1965] as it takes only $\mathcal{O}(NlogN)$ steps.
- As a unitary matrix F_N can be interpreted as a quantum operation (n-qubit unitary), i.e., mapping an N-dimensional vector of amplitudes to another N-dimensional vector of amplitudes, and called the **quantum Fourier transform (QFT)**.

- The QFT is an implementation of

$$\mathbf{U}_{FT} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi\imath \frac{kj}{N}} |k\rangle \,,$$

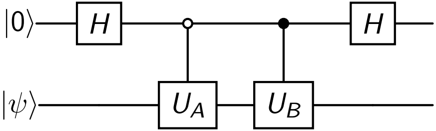
  where $N = 2^n$, using a quantum circuit with $\mathcal{O}(n^2)$ elementary gates (2-qubit SWAP and controlled rotation gates) and no ancilla quibits, which is exponentially faster than the FFT.

- The **QFT provides only the amplitudes of the resulting states**, not directly the entries of the Fourier transform.

- For more details check [Coppersmith, 2002, Nielsen and Chuang, 2001, Hales and Hallgren, 2000, Weinstein et al., 2001, Camps et al., 2021].

Linear Combination of Unitaries (LCUs) [Berry et al., 2015a]

Goal: given a few block-encoded matrices, we often need a block encoding of their linear combination, i.e., given block encodings $\mathbf{U}_A$ and $\mathbf{U}_B$ of two matrices $\mathbf{A}$ and $\mathbf{B}$, respectively, a block encoding of $\mathbf{A} + \mathbf{B}$ is given by the circuit



Now suppose we wish to implement a unitary $\mathbf{V}$ that can be written as a linear combination of many unitary gates $\mathbf{U}_i$, i.e.,

$$\mathbf{V} = \sum_i a_i \mathbf{U}_i,$$

where the unitaries $\mathbf{U}_i$ are considered easy to perform in the model under consideration (e.g., query complexity or gate complexity).

LCU Lemma [Kothari, 2014, Berry et al., 2015a]

Lemma 8 (**Exact LCU Algorithm [Kothari, 2014]**)

Let $\mathbf{V}$ *be a unitary matrix such that* $\mathbf{V} = \sum_{i \in \mathcal{I}} a_i \mathbf{U}_i$ *is a linear combination of unitary matrices* $\mathbf{U}_i$ *with* $a_i > 0$ *for all* i*. Let* $\mathbf{A}$ *be a unitary matrix that maps* $|0^m\rangle$ *to* $\frac{1}{\sqrt{a}} \sum_i \sqrt{a_i} |i\rangle$*, where* $a := \|\vec{a}\|_1 = \sum_i a_i$*. Then there exists a quantum algorithm that performs the map* $\mathbf{V}$ *exactly with* $\mathcal{O}(a)$ *uses of* $\mathbf{A}$*,* $\mathbf{U} := \sum_i |i\rangle\langle i| \otimes \mathbf{U}_i$*, and their inverses.*

Lemma 9 (**Approximate LCU algorithm)**

Let $\widetilde{\mathbf{V}}$ *be a matrix that is* δ*-close to some unitary in spectral norm, such that* $\widetilde{\mathbf{V}} = \sum_i a_i \mathbf{U}_i$ *is a linear combination of unitary matrices* $\mathbf{U}_i$ *with* $a_i > 0$ *for all* i*. Let* $\mathbf{A}$ *be a unitary matrix that maps* $|0^m\rangle$ *to* $\frac{1}{\sqrt{a}} \sum_i \sqrt{a_i} |i\rangle$*, where* $a := \|\vec{a}\|_1 = \sum_i a_i$*. Then there exists a quantum algorithm that performs the map* $\widetilde{\mathbf{V}}$ *with error* $\mathcal{O}(a\sqrt{\delta})$ *and makes* $\mathcal{O}(a)$ *uses of* $A, \mathbf{U} := \sum_i |i\rangle\langle i| \otimes \mathbf{U}_i$*, and their inverses.*

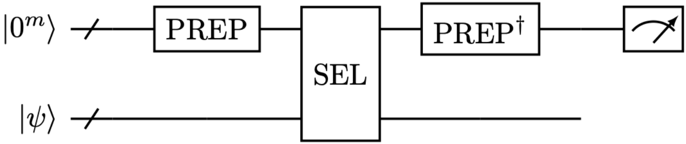
From LCU Lemmma to Quantum Circuit

LCU [Berry et al., 2015a] We can get a $(\|c\|_1, \lceil \log_2 K \rceil)$-block-encoding using:

- select oracle $\mathrm{SEL} := \sum_{i\in[K]} |i\rangle\langle i| \otimes \mathbf{U}_i$
- prepare oracle $\mathrm{PREP}\,|0\rangle = \frac{1}{\sqrt{\|c\|_1}} \sum_{i\in[K]} \sqrt{c_i}|i\rangle$,

where $K > 2^m$.

General LCBE [Gilyén et al., 2019] $\max_i m_i + \lceil \log_2 K \rceil$ ancillas.



- The LCU lemma states that the **number of ancilla qubits needed depends algorithmically of the number of terms** in the linear combination of unitaries
- Significant overhead in terms of the number of ancilla qubits needed, procedure requires implementing a sequence of sophisticated **multi-qubit controlled-unitary operations** (challenging for intermediate-term quantum computers).
- For implementing any Linear Combination of Unitaries see [Chakraborty, 2024].

Quantum Phase Estimation (QPE) [Kitaev et al., 2002]

Task: Suppose we can apply a unitary $\mathbf{U}$ and we are given an eigenvector $|\psi\rangle$ of $\mathbf{U}$ corresponding to the unknown eigenvalue λ. Our goal is to compute or at least approximate the λ.

- Quantum algorithm to estimate the phase corresponding to an eigenvalue of a given unitary operator (eigenvalues of a unitary operator have unit modulus, hence they are characterized by their phase),
- Algorithm that operates on two sets of qubits (registers) containing n and d qubits, respectively,
- We assume oracular access to the unitary operator $\mathbf{U}$ and a quantum state $|\psi\rangle$
- The cost of the algorithm is considered to be only the number of times $\mathbf{U}$ needs to be used (not the cost of implementing $\mathbf{U}$).

(imaginary) Hadamard test: estimating the real and imaginary part of $\langle\psi| U |\psi\rangle$, needs $\mathcal{O}(1/\varepsilon^2)$ measurements to estimate θ to precision ε.

Kitaev's method: uses 1 ancilla qubit, but d different circuits of various depths to estimate θ bit-by-bit,

QFT approach: one signal quantum circuit, but d ancilla qubits to store the phase information.

Quantum Phase Estimation (QPE)

Let **U** be a unitary operator acting on the d-qubit register. If $|\psi\rangle$ is an eigenvector of **U**, then

$$\mathbf{U}\,|\psi\rangle = e^{2\pi\imath\theta}\,|\psi\rangle \quad \text{for some} \quad 0 \le \theta < 1.$$

The goal of QPE is to obtain a good approximation of θ with a small number of gates and a high probability of success. The (ideal) QPE algorithm is to find $\mathbf{U}_{\mathrm{QPE}}$ (a quantum circuit) that performs transformation

$$\mathbf{U}_{\mathrm{QPE}}\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\theta\rangle\,,$$

where $|\theta\rangle = |\theta_{d-1}\rangle \cdots |\theta_1\rangle\,|\theta_0\rangle$ with binary representation $(.\theta_0\theta_1\cdots\theta_{d-1})$ of θ. We can then measure the second register (qubit) to obtain θ.

Kitaev's Idea: use a more complex quantum circuit (and in particular, with a larger circuit depth) to reduce the total number of queries. Instead of estimating θ from a single number, we assume access to U^{2^j}, and estimate θ bit-by-bit Total cost of Kitaev's method **Kitaev (1995)** (in terms of queries to U is $\mathcal{O}(\varepsilon^{-1})$.

Outline

Fundamental NLA Problems in Scientific Computing

Solving Linear Systems

Given an nonsingular $N \times N$ matrix $\mathbf{A}$ and vector $\mathbf{b}$ of size N find $\mathbf{x}$ such that

$$\mathbf{A}\mathbf{x} = \mathbf{b} \text{ or equivalently } \mathbf{x} = \mathbf{A}^{-1}\mathbf{b}.$$

Solving Least-Squares Problem

Given an $N \times N$ matrix $\mathbf{A}$ and vector $\mathbf{b}$ of size N find $\mathbf{x}$ such that

$$\min \|\mathbf{A}\mathbf{x} - \mathbf{b}\|_2.$$

Solving Eigenvalue Problem

Given an $N \times N$ matrix $\mathbf{A}$ find $\mathbf{x} \neq 0$ and $\lambda \in \mathbb{R}$ such that

$$\mathbf{A}\mathbf{x} = \lambda\mathbf{x}.$$

Functions of Matrices

Given an nonsingular (Hermitian for simplicity) $N \times N$ matrix $\mathbf{A}$ find

$$\mathbf{f}(\mathbf{A}).$$

Matrix Functions - Hermitian Matrices

Many scientific computing tasks can be expressed using matrix functions, e.g.,

solving linear systems of equation: $f(\mathbf{A}) = \mathbf{A}^{-1}$,

Gibbs state preparation: $f(\mathbf{A}) = e^{-\beta \mathbf{A}}$, or

Hamiltonian simulation: $f(\mathbf{A}) = e^{\imath i \mathbf{A} t}$.

Goal: construct an efficient quantum circuit to compute $f(\mathbf{A}) |b\rangle$ for any state $|b\rangle$.

Idea: qubitization [Low and Chuang, 2019].

Definition 10 (**Matrix function of Hermitian matrices**)

Let $\mathbf{A} \in \mathbb{C}^{N \times N}$ be an *n*-qubit Hermitian matrix with eigenvalue decomposition

$$\mathbf{A} = \mathbf{V} \Lambda \mathbf{V}^*,$$

where $\Lambda = \operatorname{diag}(\lambda_0, \ldots, \lambda_{N-1})$ is a diagonal matrix with $\lambda_0 \leq \cdots \leq \lambda_{N-1}$ being the eigenvalues of $\mathbf{A}$. Let $f : \mathbb{R} \to \mathbb{C}$ be a scalar function such that $f(\lambda_i)$ is defined for all $i = 0, \ldots, N-1$. Then the matrix function $f(A)$ can be defined in terms of this eigendecomposition as

$$\mathbf{f}(\mathbf{A}) := \mathbf{V} f(\Lambda) \mathbf{V}^*,$$

where

$$f(\Lambda) = \operatorname{diag}(f(\lambda_0), f(\lambda_1), \ldots, f(\lambda_{N-1})).$$

Qubitization for representing matrix functions

Let us first introduce the main idea behind qubitization using a simple example. For any $-1 < \lambda \leq 1$, we can consider a 2×2 rotation matrix

$$\mathbf{O}(\lambda) = \begin{bmatrix} \lambda & \sqrt{1-\lambda^2} \\ -\sqrt{1-\lambda^2} & \lambda \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix},$$

with the change of variable $\lambda = \cos\theta, 0 \leq \theta < \pi$. Direct computations yield

$$\mathbf{O}^k(\lambda) = \begin{bmatrix} \cos(k\theta) & \sin(k\theta) \\ -\sin(k\theta) & \cos(k\theta) \end{bmatrix} = \begin{bmatrix} T_k(\lambda) & \sqrt{1-\lambda^2}U_{k-1}(\lambda) \\ -\sqrt{1-\lambda^2}U_{k-1}(\lambda) & T_k(\lambda) \end{bmatrix},$$

with

$$T_k(\lambda) = \cos(k\theta) = \cos(k \arccos\lambda), \quad U_{k-1}(\lambda) = \frac{\sin(k\theta)}{\sin\theta} = \frac{\sin(k\arccos\lambda)}{\sqrt{1-\lambda^2}},$$

being the Chebyshev polynomials of first and second kind, respectively.

If we can "replace" λ by $\mathbf{A}$, we obtain a (1,1)-block-encoding for the Chebyshev polynomial $T_k(\mathbf{A})$.

In the following we will assume that $\mathbf{A}$ is queried in the exact block-encoding model, i.e., $\mathbf{U}_A$ is an $(1, m)$-block-encoding of matrix $\mathbf{A}$. Let us consider the eigendecomposition

$$\mathbf{A} = \sum_i \lambda_i |v_i\rangle \langle v_i| .$$

Then, since $\mathbf{A} = (\langle 0|^{\otimes m} \otimes I_n)\mathbf{U}_A(|0\rangle^{\otimes m} \otimes I_n)$, for each eigenstate $|v_i\rangle$,

$$\mathbf{U}_A |0^m\rangle |v_i\rangle = |0^m\rangle \mathbf{A} |v_i\rangle + \left|\widetilde{\perp}_i\right\rangle = \lambda_i |0^m\rangle |v_i\rangle + \left|\widetilde{\perp}_i\right\rangle , \tag{4}$$

where $\left|\widetilde{\perp}_i\right\rangle$ denotes an unnormalized state orthogonal to all states of the form $|0^m\rangle |\psi\rangle$, i.e., given a projection operator $\Pi = |0^m\rangle \langle 0^m| \otimes I_n$

$$\Pi \left|\tilde{\perp}_i\right\rangle = 0.$$

Using a normalized state $|\perp_i\rangle$ we can write

$$\left|\widetilde{\perp}_i\right\rangle = \sqrt{1 - \lambda_i^2} |\perp_i\rangle . \tag{5}$$

Hence, (4) can be written as

$$\mathbf{U}_A |0^m\rangle |v_i\rangle = \lambda_i |0^m\rangle |v_i\rangle + \sqrt{1-\lambda_i^2} |\perp_i\rangle .$$

If we now formally denote

$$|0\rangle^{\otimes m} |v_i\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |\perp_i\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

we can write

$$\mathbf{U}_A \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \lambda_i \\ \sqrt{1-\lambda_i^2} \end{bmatrix}. \quad (6)$$

Since $\mathbf{U}_A$ is unitary and Hermitian, $\mathbf{U}_A^2 = I$. From this and (6), it follows that

$$\mathbf{U}_A = \begin{bmatrix} \lambda_i & \sqrt{1-\lambda_i^2} \\ \sqrt{1-\lambda_i^2} & -\lambda_i \end{bmatrix}, \quad (7)$$

which is a **reflection matrix**.

With change of variable $\lambda_i = cos(\theta_i), 0 \leq \theta_i < \pi$

$$\mathbf{U}_A = \begin{bmatrix} cos(\theta_i) & sin(\theta_i) \\ sin(\theta_i) & -cos(\theta_i) \end{bmatrix}. \tag{8}$$

As our goal is to get the block-encoding of $T_k(\mathbf{A})$, we want to transform $\mathbf{U}_A$ into a rotation matrix $\mathbf{O}(\lambda)$. Note that this is possible if we can flip the signs of the entries in the second row of $\mathbf{U}_A$, i.e., multiply $\mathbf{U}_A$ on the left by $\mathbf{R}_\Pi$ such that

$$\begin{aligned} \mathbf{R}_\Pi \mathbf{U}_A &= \mathbf{R}_\Pi \begin{bmatrix} \lambda_i & \sqrt{1-\lambda_i^2} \\ \sqrt{1-\lambda_i^2} & -\lambda_i \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \lambda_i & \sqrt{1-\lambda_i^2} \\ \sqrt{1-\lambda_i^2} & -\lambda_i \end{bmatrix} \\ &= \begin{bmatrix} \lambda_i & \sqrt{1-\lambda_i^2} \\ -\sqrt{1-\lambda_i^2} & \lambda_i \end{bmatrix} = \begin{bmatrix} cos(\theta_i) & sin(\theta_i) \\ -sin(\theta_i) & cos(\theta_i) \end{bmatrix} = \mathbf{O}. \end{aligned} \tag{9}$$

Note that $\mathbf{R}_\Pi = 2\Pi - \mathbf{I}$, acts as a reflection operator restricted to each subspace $\mathcal{H}_i$. Hence,

$$\mathbf{O}^k = (\mathbf{R}\mathbf{U}_A)^k = \begin{bmatrix} T_k(\mathbf{A}) & * \\ * & * \end{bmatrix}, \tag{10}$$

is a $(1, m)$-block-encoding of the Chebyshev polynomial $T_k(\mathbf{A})$. If $m = 1$, then $\mathbf{R}_\Pi$ is just the Pauli $\mathbf{Z}$ gate. For $m > 1$, the circuit

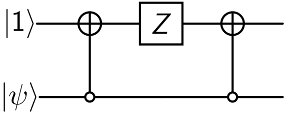


Figure 12: Circuit for rotation operator O.

returns $|1\rangle\,|0^m\rangle$ if $\psi = 0^m$, and $-|1\rangle|\psi\rangle$ if $\psi \neq 0^m$. Hence, it implements $\mathbf{R}_\Pi$ with the signal qubit $|1\rangle$ used as a work register. Altenatively, we may discard the signal qubit, and denote resulting unitary by $\mathbf{R}_\Pi$.

Since cicuit in Figure 12 implements the operator $\mathbf{O}$ repeating it k times gives the $(\ 1, m+1\ )$-block-encoding of $T_k(\mathbf{A})$, i.e.,

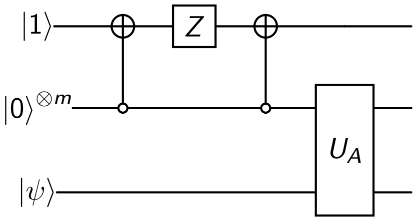


Figure 13: Circuit for one step of qubitization with a Hermitian $(1, m)$-block-encoding $\mathbf{U}_A$ of Hermitian matrix $\mathbf{A}$.

Quantum Linear System Problem (QLSP)

Classical Linear System Problem: Given an nonsingular (Hermitian for simplicity) $N \times N$ matrix $\mathbf{A}$ and vector $\mathbf{b}$ of size N find x such that

$$\mathbf{A}\mathbf{x} = \mathbf{b} \quad \text{or equivalently} \quad \mathbf{x} = \mathbf{A}^{-1}\mathbf{b}.$$

Best general purpose algorithm **Conjugate Gradient (CG)** method has **asymptotic complexity** $\mathcal{O}(N\sqrt{\kappa(\mathbf{A})}$.

Quantum Linear System Problem (QLSP): Given an nonsingular $N \times N$ matrix $\mathbf{A}$ and a quantum state $|b\rangle$ of size N find (prepare) a quantum state $|\widetilde{x}\rangle$ such that

$$\| \, |\widetilde{x}\rangle - |x\rangle \, \| \leq \varepsilon \quad \text{and} \quad |x\rangle = \frac{\mathbf{A}^{-1} \, |b\rangle}{\|\mathbf{A}^{-1} \, |b\rangle \, \|}.$$

$|\widetilde{x}\rangle$ **is an ε-approximation** of a quantum state $|x\rangle$.

QLSP Assumptions

- There **exists a black-box procedure to compute the elements of matrix** $\mathbf{A}$, e.g., block-encoding.
- There **exists a black-box procedure to prepare the initial state** $|b\rangle$, i.e., $|b\rangle = \mathbf{U}_b |0^n\rangle$ (we assume they can be implemented using two-qubit gates in "constant" time).
- The number of uses of the procedures determines query complexity of the algorithm, the number of queries provides a lower bound for the gate complexity.

Remark 11

This quantum version of the problem is, however, only useful for computing expectation values in the solution of the system, but not for obtaining the actual solution vector.

Query Complexity for QLSP

Harrow, Hasidim, Lloyd (2008) Quantum Phase Estimation (QPE), $\widetilde{\mathcal{O}}(\kappa^2(A) log(N)/\varepsilon$

Ambainis (2012) Variable Time Amplitude Amplification (VTAA), $\widetilde{\mathcal{O}}(\kappa(A) log(N)/\varepsilon^3$

Childs, Kothari, Somma (2017) LCU, Chebyshev approximation, $\widetilde{\mathcal{O}}(\kappa(A) log(N) poly\ log(1/\varepsilon)$

Subasi, Somma, Orsucci (2018) Adiabatic Quantum Computing (AQC), $\widetilde{\mathcal{O}}(\kappa(A) log(N)/\varepsilon)$

An and Lin (2019) Time-optimal Adiabatic Quantum Approach (AQC), $\mathcal{O}(\kappa(A) log(N)/\varepsilon)$

Harrow, Hasidim, and Lloyd (HHL) Algorithm [Harrow et al., 2009]

Goal: prepare a quantum state $|x\rangle$ whose amplitudes are equal to the elements of the vector x that solves $\mathbf{Ax} = \mathbf{b}$ for symmetric positive definite $\mathbf{A}$.

- the first quantum algorithm for solving QLSP,
- gives a **scalar measurement on the solution vector**, instead of the values of the solution vector itself,
- implements a $1/\kappa(A)$**-approximation to the initial state**,
- its complexity is $\approx (\kappa(\mathcal{A})/\varepsilon)$, i.e., $\widetilde{\mathcal{O}}(\kappa^2 log(N)/\varepsilon)$,

Consider the eigendecomposition of a sparse, nonsingular $\mathbf{A}$ with $\kappa(\mathbf{A}) < \infty$, i.e.,

$$\mathbf{A} |v_j\rangle = \lambda_j |v_j\rangle, j = 0, \dots, N-1,$$

with eigenvalues $0 < \lambda_0 \leq \lambda_1 \leq \dots \lambda_{N-1} < 1$ having an exact d-bit representation.

HHL Procedure

Step 1 Use Hamiltonian simulation technique to transform matrix $\mathbf{A}$ into a unitary operator $\mathbf{U} = e^{\imath 2\pi \mathbf{A}}$ that can be applied to $|b\rangle$, i.e.,

if $|b\rangle = |v_j\rangle$ then QPE can be applied to implement

$$\mathbf{U}_{\mathrm{QPE}} \left|0^d\right\rangle |v_j\rangle = |\lambda_j\rangle |v_j\rangle .$$

else expand the input state $|b\rangle = \sum_{j=0}^{N-1} \beta_j |v_j\rangle$ and

$$\mathbf{U}_{\mathrm{QPE}} \left|0^d\right\rangle |v_j\rangle = \sum_{j=0}^{N-1} \beta_j |\lambda_j\rangle |v_j\rangle .$$

Step 2 Since the unnormalized solution satisfies

$$\mathbf{A}^{-1}|b\rangle = \left(\sum_{j=0}^{N-1} \lambda_j^{-1} |v_j\rangle \langle v_j|\right)\left(\sum_{j=0}^{N-1} \beta_j |v_j\rangle\right) = \sum_{j=0}^{N-1} \frac{\beta_j}{\lambda_j} |v_j\rangle,$$

we will need to use the information on the eigenvalues $|\lambda_j\rangle$ stored in the ancilla register and perform a controlled rotation to multiply the factor λ_j^{-1} to each β_j.

Example Quantum Eigenvalue Problem

Classical Eigenvalue Problem: Given an nonsingular (Hermitian for simplicity) $N \times N$ matrix $\mathbf{A}$ and vector of size N find $\lambda \in \mathbb{R}$ and a nonzero vector $x \in \mathbb{R}^N$ such that

$$\mathbf{A}\mathbf{x} = \lambda \mathbf{x}.$$

Example Quantum Eigenvalue Problem: Given a Hamiltonian $\mathcal{H} = \sum_{i=0}^{T} \alpha_i \mathbf{P}_i$, where $\alpha_i \in \mathbb{R}_+$, $\sum_{i=0}^{T-1} \alpha_i = 1$, $\mathbf{P}_i$ are Pauli operators and $T = \mathcal{O}(poly(n))$, find (prepare) a ground state $|\widetilde{x}\rangle$ such that

$$\mathcal{H} |\psi\rangle = E_0 |\psi\rangle,$$

where $|\psi\rangle$ is a ground state (state corresponding to the lowest energy E_0.

Quantum Subspace Diagonalization (QSD) [Cortes and Gray, 2022b, Epperly et al., 2022]

Given a set of states

$$\{|\psi_k\rangle = \mathbf{U}_k |\psi_0\rangle, \quad k = 0, 1, 2, \ldots, D-1\} \tag{11}$$

that can be prepared on a quantum computer by quantum circuits $\mathbf{U}_k$, we project the Hamiltonian $\mathcal{H}$ onto the D-dimensional Hilbert space $\text{span}\{|\psi_k\rangle = U_k |\psi_0\rangle, k = 0, 1, 2, \ldots, D-1\}$, i.e.,

$$\begin{aligned} \mathbf{H}_{ij} &= \langle\psi_i| H |\psi_j\rangle = \langle\psi_0| U_i^* H U_j |\psi_0\rangle, \\ \mathbf{S}_{ij} &= \langle\psi_i \mid \psi_j\rangle = \langle\psi_0| U_i^{*,} U_j |\psi_0\rangle. \end{aligned} \tag{12}$$

Then, having estimated $\mathbf{H}$ and $\mathbf{S}$, we classically solve the generalized eigenvalue problem (GEVP)

$$\mathbf{H}\mathbf{v} = \mu \mathbf{S}\mathbf{v} \tag{13}$$

and find the lowest eigenvalue μ, variational estimate of the ground state energy.

Remark 12

- $\mathbf{S}$ *is the overlap (Gram) matrix of the states* (11)*,*
- $\mathbf{H}$ *and* $\mathbf{S}$ *can be estimated by repeated SWAP or Hadamard tests,*
- *generalized eigenvalue problem* (13) *needs to be regularized due to ill-conditioning of* $\mathbf{S}$ *with growing* D*.*

Classical Lanczos Method

Input: Hamiltonian $\mathcal{H}$ and initial guess $|\psi_0\rangle$

$\Rightarrow$ $\mathcal{H}|\psi_0\rangle \Rightarrow \cdots \Rightarrow \mathcal{H}^{D-1}|\psi_0\rangle$

$(\mathbf{H}, \mathbf{S})$ = project $\mathcal{H}$ onto span

$$\underbrace{\left\{ |\psi_0\rangle, \mathcal{H}|\psi_0\rangle, \mathcal{H}^2|\psi_0\rangle, \ldots, \mathcal{H}^{D-1}|\psi_0\rangle \right\}}_{\text{Krylov space}}$$

Output: Lowest eigenvalue of $(\mathbf{H}, \mathbf{S})$ (Ritz value), i.e., $\mathbf{Hv} = \mu\mathbf{Sv}$, approximates lowest eigenvalue of $\mathcal{H}$

Advantages:

- Exponential convergence with respect to D (in infinite precision arithmetic).

Disadvantages:

- Requires storing Krylov basis vectors, $\mathcal{H}^k|\psi_0\rangle$ exponential overhead (cost of classically representing vectors).

Is it possible to design a quantum version that reduces statevector overhead while maintaining rapid convergence?

Towards Quantum Lanczos

Several quantum methods have been proposed to adapt the Lanczos algorithm:

imaginary time evolution approaches: Quantum Lanczos (QLanczos) [Motta et al., 2020],

real time evolution approaches : Quantum Filter Diagonalization (QFD) [Parrish and McMahon, 2019, Stair et al., 2020, Cohn et al., 2021], [Cortes and Gray, 2022a, Klymko et al., 2022],

linear combinations of time evolutions: Quantum Power Method [Seki and Yunoki, 2021] approximates powers of H via linear combinations of time-evolved states.

- All these methods converge to the classical Lanczos algorithm in specific limits.
- However, both real and imaginary time evolution require approximations.

Truly Quantum Lanczos [Kirby et al., 2023]

- A **quantum algorithm** that produces **exactly the same Krylov space** as the one used in the **classical Lanczos method** (up to finite sampling noise).
- Focuses on **Hamiltonians encoded as linear combinations of Pauli operators**, which simplifies the measurement scheme, however, the method is **generalizable to other block encodings**.
- The **Krylov basis vectors** are defined using **Chebyshev polynomials**:

$$|\psi_k\rangle = T_k(H)|\psi_0\rangle \quad \text{for } k = 0, 1, \ldots, D-1.$$

- Since **Chebyshev polynomials span the same space as powers of H**, we have:

$$\text{span}\{T_k(H)|\psi_0\rangle\} = \text{span}\{H^k|\psi_0\rangle\}.$$

- The **quantum subspace diagonalization (QSD) approach** can find the **lowest-energy state** in this Krylov subspace.
- Thus, using Chebyshev polynomials yields **performance equivalent to powers of the Hamiltonian**, up to **finite sample noise**.

QSD step in Quantum Lanczos

To diagonalize $\mathcal{H}$ projected onto subspace span$\{T_k(H)|\psi_0\rangle\}_{k=0}^{D-1}$, we need to estimate

$$\mathbf{H}_{ij} := \langle\psi_0|\, T_i(H) H T_j(H)\, |\psi_0\rangle\,, \quad \mathbf{S}_{ij} := \langle\psi_0|\, T_i(H) T_j(H)\, |\psi_0\rangle$$

on quantum computer for $i, j = 0, 1, 2, \ldots, D-1$, then solve a generalized eigenvalue problem

$$\mathbf{Hv} = \mu\mathbf{Sv}.$$

Using the block encodings of $T_k(\mathcal{H})\,|\psi_0\rangle$, the properties of Chebyshev polynomials and denoting by $\langle\cdot\rangle_0$ expectation value with respect to the initial state $|\psi_0\rangle$ we get:

$$\mathbf{H}_{ij} = \langle T_i(\mathcal{H})\mathcal{H}T_j(\mathcal{H})\rangle_0 = \frac{1}{4}\Big(\langle T_{i+j+1}(\mathcal{H})\rangle_0 + \langle T_{|i+j-1|}(\mathcal{H})\rangle_0 + \langle T_{|i-j+1|}(\mathcal{H})\rangle_0 + \langle T_{|i-j-1|}(\mathcal{H})\rangle_0\Big)\,.$$

$$\mathbf{S}_{ij} = \langle T_i(\mathcal{H}) T_j(\mathcal{H}) \rangle_0 = \frac{1}{2} \left(\langle T_{i+j}(\mathcal{H}) \rangle_0 + \langle T_{|i-j|}(\mathcal{H}) \rangle_0 \right),$$

for $i, j = 0, 1, 2, \ldots, D-1$.

Therefore, to construct matrices $\mathbf{H}$ and $\mathbf{S}$, we only need to estimate all expectation values

$$\langle T_k(\mathcal{H}) \rangle_0 := \langle \psi_0 | \, T_k(\mathcal{H}) \, | \psi_0 \rangle \quad \text{for} \quad k = 0, 1, 2, \ldots, 2D-1.$$

Let us now recall the Definition 6 of the standard form

$$(\langle G|_a \otimes \mathbf{I}_s) \, \mathbf{U}_H \, (|G\rangle_a \otimes \mathbf{I}_s) = \mathcal{H} \; . \tag{14}$$

and our simple n-qubit Hamiltonian expressed as a linear combination of Pauli operators $\mathbf{P}_i$, $i = 1, \ldots, T$, $T = \mathcal{O}(poly(n))$, i.e.,

$$\mathcal{H} = \sum_{i=0}^{T-1} \alpha_i P_i.$$

Block-Encoding and Implementation of the Unitary Then the block-encoding $\mathbf{U}_H$ of the Hamiltonian $\mathcal{H}$ is given as

$$\mathbf{U}_H = \sum_{i=0}^{T-1} |i\rangle_a \langle i|_a \otimes \mathbf{P}_i.$$

- Apply $P_i^{(j)}$ (the j^{th} single-qubit Pauli operator in $\mathbf{P}_i$) to system qubit j, controlled on the auxiliary qubits being in state $|\ i)_\alpha$.
- As P_i is an n-qubit Pauli operator, implementing $\mathbf{U}_H$ requires applying at most nT single-qubit Pauli operators, each controlled on all of the auxiliary qubits.

Block-encoding and Preparation Procedure for the State

$$|G\rangle_a = \sum_{i=0}^{T-1} \sqrt{\alpha_i}\, |i\rangle_a .$$

We can use any existing state preparation procedures for $|G\rangle_a = G|0\rangle_a$ since there are only logarithmically-many auxiliary qubits, so it is efficient.

Getting $\langle T_k(\mathcal{H}) \rangle_0$ from $(\mathbf{U}_H, G)$

Lemma 13 (**Chebyshev polynomials from block-encoding [Kirby et al., 2023]**)

Given $(\mathbf{U}_H, G)$ *of a Hamiltonian* $\mathcal{H}$*, such that* $\mathbf{U}_H^2 = \mathbf{I}$*, let*

$$\mathbf{R} := (2|G\rangle_a \langle G|_a - \mathbf{I}_a) \otimes \mathbf{I}_s \,.$$

be the reflection around $|G\rangle_a$ *in the auxiliary space. Then*

$$\Big(\langle G|_a \otimes \mathbf{I}_s) (RU)^k (|G\rangle_a \otimes \mathbf{I}_s) = T_k(\mathcal{H}) \,.$$

for any $k = 0, 1, 2, \ldots$*, where* $T_k(\cdot)$ *is the* k*th Chebyshev polynomial of the first kind, i.e.,* $(\mathbf{RU}_H)^k$ **is a block encoding of** $T_k(\mathcal{H})$.

$$\mathbf{U}_H = \begin{bmatrix} \mathcal{H} & \cdot \\ \cdot & \cdot \end{bmatrix}, \quad \mathbf{R}_H = \begin{bmatrix} \mathbf{I} & 0 \\ 0 & -\mathbf{I} \end{bmatrix}$$

With $\mathbf{U}_H^2 = I$

$$(\mathbf{R}\mathbf{U}_H)^k = \begin{bmatrix} T_k(\mathcal{H}) & \cdot \\ \cdot & \cdot \end{bmatrix}.$$

- Given a **block-encoding** $(\mathbf{U}_H, G)$ of a Hamiltonian $\mathcal{H}$, Lemma 13 leads to:

$$\langle T_k(\mathcal{H})\rangle_0 = (\langle G|_a \otimes \langle\psi_0|)\,(\mathbf{RU})^k\,(|G\rangle_a \otimes |\psi_0\rangle)$$

- Since $\mathbf{R}$ is a Hermitian **reflection about** $|G\rangle_a$, the expression simplifies:

$$\langle T_k(H)\rangle_0 = (\langle G|_a \otimes \langle\psi_0|)\,U(RU)^{k-1}\,(|G\rangle_a \otimes |\psi_0\rangle)\,.$$

- The operator $(\mathbf{U}_H(\mathbf{RU}_H)^{k-1})$ can be rewritten based on the parity of k:

$$\mathbf{U}_H(\mathbf{RU}_H)^{k-1} = \begin{cases} (\mathbf{U}_H\mathbf{R})^{k/2}\mathbf{R}(\mathbf{RU}_H)^{k/2} & \text{if } k \text{ is even} \\ (\mathbf{U}_H\mathbf{R})^{\lfloor k/2\rfloor}\mathbf{U}_H(\mathbf{RU}_H)^{\lfloor k/2\rfloor} & \text{if } k \text{ is odd.} \end{cases}$$

Hence, defining the state

$$\left|\psi_{\lfloor k/2 \rfloor}\right\rangle = (\mathbf{R}\mathbf{U}_H)^{\lfloor k/2 \rfloor} \left(|G\rangle_a \otimes |\psi_0\rangle \right),$$

and its adjoint

$$\left\langle \psi_{\lfloor k/2 \rfloor}\right| = \Big(\langle\, G|_a \otimes \langle \psi_0| \right) (\mathbf{U}_H\mathbf{R})^{\lfloor k/2 \rfloor}$$

yields

$$\langle T_k(\mathcal{H}) \rangle_0 = \begin{cases} \langle \psi_{\lfloor k/2 \rfloor} | \mathbf{R} | \psi_{\lfloor k/2 \rfloor} \rangle & \text{if } k \text{ is even,} \\ \langle \psi_{\lfloor k/2 \rfloor} | \mathbf{U}_H | \psi_{\lfloor k/2 \rfloor} \rangle & \text{if } k \text{ is odd.} \end{cases}$$

Measurement Procedure

1. **State preparation:** Prepare $|\psi_{\lfloor k/2 \rfloor}\rangle$ by applying RU $\lfloor k/2 \rfloor$ times to $|G\rangle_a \otimes |\psi_0\rangle$.
2. **If k is even** (measure R):
   - Apply $G^\dagger$ to undo G.
   - Measure observable $2|0\rangle_a\langle 0|_a - 1$ on the auxiliary qubits.
   - Return $+1$ if all auxiliary qubits are measured as $|0\rangle$; otherwise return -1.
3. **If k is odd** (measure U):
   - Decompose $U = \sum_i |i\rangle_a\langle i|_a \otimes P_i$.
   - Measure auxiliary qubits in the computational basis.
   - If the result is $|i\rangle_a$, measure system qubits in the Pauli basis P_i; otherwise return 0.
4. **Repeat** steps 1–3 until enough statistics are collected to estimate the expectation value to the desired precision.

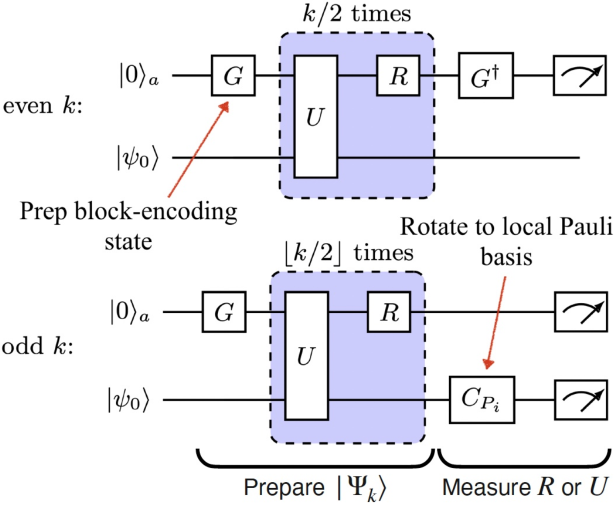


Figure 14: [Kirby et al., 2023]

Summary of Requirements and Costs

Block Encoding $(\mathbf{U}_H, G)$: for n qubits and T Hamiltonian terms:

- Cost of $\mathbf{U}_H$: nT
- Cost of G: $2T$
- Cost of $\mathbf{R}$: $4T$

All in $\lceil \log_2 T \rceil$-controlled single-qubit gates

Measurement Overhead: depends on the target precision and the classical methods used to regularize and solver the generalized eigenvalue problem

State Preparation:

- Prepare $|G\rangle_a \otimes |\psi_0\rangle$
- Apply up to $D-1$ layers of $\mathbf{RU}_H$
- Measure either in Pauli basis or apply $G^\dagger$ then measure
- Longest sequence uses $(D-1)nT + 4DT$ $\lceil \log_2 T \rceil$-controlled single-qubit gates.

Qubit Requirements:

- system qubits for $|\psi_0\rangle$ (those that $\mathcal{H}$ acts on),
- auxiliary qubits for $|G\rangle_a$: can be $\lceil \log_2 T \rceil$ if Hamiltonian has T terms

Error Analysis of Quantum Lanczos

Error scaling subject to:

- finite sample noise, i.e., matrix elements are obtained from expectations values estimated by repeated measurements)
- devise noise, when executing the algorithm on a real quantum computer,
- regularization of the overlap matrix **S**, stability issues, condition number of **S** grows exponentialy with the Krylov space dimension D

Ground State Energy Estimate

Theorem 14 (Theorem 1, [Kirby et al., 2023])

The error in the ground state energy estimate coming from the regularized problem ... is bounded by

$$\mathcal{E} \leq \mathcal{O}(\left(D^4\eta\right)^{\frac{1}{1+\alpha}} + \frac{\sqrt{\delta}\epsilon_{total}}{|\gamma_0|^2} + \delta + \frac{1}{|\gamma_0|^2}\left(1+\frac{\delta}{2}\right)^{-D},)$$

with

η noise rate,

$0 \leq \alpha \leq 1/2$ constant ($\alpha = 1/4$ [Epperly et al., 2022] and $\alpha = 0$ [Kirby et al., 2023]),

$\delta > 0$ constant,

$\epsilon > 0$ threshold for regularization,

ϵ_{total} sum of the eigenvalues of **S** discarded by regularization,

γ_0 overlap of the initial reference state $|\psi_0\rangle$ with the true grounds state $|E_0\rangle$, $\gamma_0 = \langle E_0|\psi_0\rangle$.

$$\mathcal{E} \leq \mathcal{O}\left(\left(D^4\eta\right)^{\frac{1}{1+\alpha}} + \frac{\sqrt{\delta}\epsilon_{\text{total}}}{|\gamma_0|^2} + \delta + \frac{1}{|\gamma_0|^2}\left(1+\frac{\delta}{2}\right)^{-D} \right)$$

Term 4 error due to exact Krylov space, vanishes exponentially with the Krylov space dimension D,

Term 3 energy error tolerance, determines the rate of exponential decay of aplitudes of energies more than δ above the ground state, if $\delta \approx \Delta$(spectral gap) this term can be removed, otherwise the approximated state in general will not be a ground state, but an arbitrary state in the low energy subspae within δ distance of the ground state energy,

Term 2 error due to regularization of $(\mathbf{H}, \mathbf{S})$ by ϵ, i.e., discarding eigenspaces of $\mathbf{S}$ with eigenvalues smaller than ϵ,

Term 1 factor $D^{\frac{4}{1+\alpha}}$ comes from the proof technique [Epperly et al., 2022].

$$\mathcal{E} \leq \mathcal{O}\left(\left(D^4\eta\right)^{\frac{1}{1+\alpha}} + \frac{\sqrt{\delta}\epsilon_{\text{total}}}{|\gamma_0|^2} + \delta + \frac{1}{|\gamma_0|^2}\left(1+\frac{\delta}{2}\right)^{-D} \right)$$

Term 4 error due to exact Krylov space, vanishes exponentially with the Krylov space dimension D,

Term 3 energy error tolerance, determines the rate of exponential decay of aplitudes of energies more than δ above the ground state, if $\delta \approx \Delta$(spectral gap) this term can be removed, otherwise the approximated state in general will not be a ground state, but an arbitrary state in the low energy subspae within δ distance of the ground state energy,

Term 2 error due to regularization of $(\mathbf{H}, \mathbf{S})$ by ϵ, i.e., discarding eigenspaces of $\mathbf{S}$ with eigenvalues smaller than ϵ,

Term 1 factor $D^{\frac{4}{1+\alpha}}$ comes from the proof technique [Epperly et al., 2022].

$$\mathcal{E} \leq \mathcal{O}\left(\left(D^4\eta\right)^{\frac{1}{1+\alpha}} + \frac{\sqrt{\delta}\epsilon_{\text{total}}}{|\gamma_0|^2} + \delta + \frac{1}{|\gamma_0|^2}\left(1+\frac{\delta}{2}\right)^{-D} \right)$$

Term 4 error due to exact Krylov space, vanishes exponentially with the Krylov space dimension D,

Term 3 energy error tolerance, determines the rate of exponential decay of aplitudes of energies more than δ above the ground state, if $\delta \approx \Delta$(spectral gap) this term can be removed, otherwise the approximated state in general will not be a ground state, but an arbitrary state in the low energy subspae within δ distance of the ground state energy,

Term 2 error due to regularization of $(\mathbf{H}, \mathbf{S})$ by ϵ, i.e., discarding eigenspaces of $\mathbf{S}$ with eigenvalues smaller than ϵ,

Term 1 factor $D^{\frac{4}{1+\alpha}}$ comes from the proof technique [Epperly et al., 2022].

$$\mathcal{E} \leq \mathcal{O}\left(\left(D^4\eta\right)^{\frac{1}{1+\alpha}} + \frac{\sqrt{\delta}\epsilon_{\text{total}}}{|\gamma_0|^2} + \delta + \frac{1}{|\gamma_0|^2}\left(1+\frac{\delta}{2}\right)^{-D} \right)$$

Term 4 error due to exact Krylov space, vanishes exponentially with the Krylov space dimension D,

Term 3 energy error tolerance, determines the rate of exponential decay of aplitudes of energies more than δ above the ground state, if $\delta \approx \Delta$(spectral gap) this term can be removed, otherwise the approximated state in general will not be a ground state, but an arbitrary state in the low energy subspae within δ distance of the ground state energy,

Term 2 error due to regularization of $(\mathbf{H}, \mathbf{S})$ by ϵ, i.e., discarding eigenspaces of $\mathbf{S}$ with eigenvalues smaller than ϵ,

Term 1 factor $D^{\frac{4}{1+\alpha}}$ comes from the proof technique [Epperly et al., 2022].

Actuall Error Bound

To reach energy error $\mathcal{E}$ we require:

Krylov space dimension: $D = \Theta\left[\left(\log\frac{1}{|\gamma_0|} + \log\frac{1}{\mathcal{E}}\right)\min\left(\frac{1}{\mathcal{E}}, \frac{1}{\Delta}\right)\right]$ (is also a maximum circuit depth in terms of queries to the block-encoding operator).

Total number of measurements: $M = \Theta\left(D(\frac{1}{\mathcal{E}^2} + \frac{1}{\mathcal{E}|\gamma_0|^4})\right)$.

Summary of [Kirby et al., 2023] Quantum Lanczos

- uses block encoding to **exactly reproduce the Krylov space of the classical Lanczos** method on quantum computer,
- this quantum algorithm **achieves it in polynomial time and memory**,
- resulting Krylov space (although not represented with orthogonal basis) is identical to the one generated by the Lanczos method (up to finite sample noise),
- this algorithm **does not require simulating real or imaginary time evolution**,
- **explicit error bounds** in the presence of noise,
- requires $\Omega(1/poly(n))$ **overlap between initial state and the true ground state** for n qubits,
- it **requires one local basis rotation per circuit** in addition to the block encoding unitaries.

Thank you very much for your attention.

Questions?

References

Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, H., Werner, R., and Zeilinger, A. (2003).
Quantum information: An introduction to basic theoretical concepts and experiments, volume 173.
Springer.

An, D. (2023).
Introduction to quantum numerical linear algebra.
IPAM Mathematical and Computational Challenges in Quantum Computing Tutorials.

Berry, D. W. and Childs, A. M. (2009).
Black-box hamiltonian simulation and unitary implementation.
arXiv preprint arXiv:0910.4157.

Berry, D. W., Childs, A. M., Cleve, R., Kothari, R., and Somma, R. D. (2015a).
Simulating hamiltonian dynamics with a truncated taylor series.
Physical review letters, 114(9):090502.

Berry, D. W., Childs, A. M., and Kothari, R. (2015b).
Hamiltonian simulation with nearly optimal dependence on all parameters.
In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 792–809.

Camps, D., Lin, L., Van Beeumen, R., and Yang, C. (2024).
Explicit quantum circuits for block encodings of certain sparse matrices.
SIAM Journal on Matrix Analysis and Applications, 45(1):801–827.

Camps, D. and Van Beeumen, R. (2020).
Approximate quantum circuit synthesis using block encodings.
Physical Review A, 102(5):052411.

Camps, D. and Van Beeumen, R. (2022).
Fable: Fast approximate quantum circuits for block-encodings.
In *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 104–113. IEEE.

Camps, D., Van Beeumen, R., and Yang, C. (2021).
Quantum fourier transform revisited.
Numerical Linear Algebra with Applications, 28(1):e2331.

Chakraborty, S. (2023).

Implementing any linear combination of unitaries on intermediate-term quantum computers.

arXiv preprint arXiv:2302.13555.

Chakraborty, S. (2024).

Implementing any linear combination of unitaries on intermediate-term quantum computers.

Quantum, 8:1496.

Chakraborty, S., Gilyén, A., and Jeffery, S. (2019).

The Power of Block-Encoded Matrix Powers: Improved Regression Techniques via Faster Hamiltonian Simulation.

In Baier, C., Chatzigiannakis, I., Flocchini, P., and Leonardi, S., editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 33:1–33:14, Dagstuhl, Germany. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

Childs, A. M. (2010).

On the relationship between continuous-and discrete-time quantum walk.

Communications in Mathematical Physics, 294:581–603.

Childs, A. M., Kothari, R., and Somma, R. D. (2017).
Quantum algorithm for systems of linear equations with exponentially improved dependence on precision.
SIAM Journal on Computing, 46(6):1920–1950.

Childs, A. M. and Wiebe, N. (2012).
Hamiltonian simulation using linear combinations of unitary operations.
arXiv preprint arXiv:1202.5822.

Cohn, J., Motta, M., and Parrish, R. M. (2021).
Quantum filter diagonalization with compressed double-factorized hamiltonians.
PRX Quantum, 2:040352.

Coppersmith, D. (2002).
An approximate fourier transform useful in quantum factoring.
arXiv preprint quant-ph/0201067.

Cortes, C. L. and Gray, S. K. (2022a).
Quantum krylov subspace algorithms for ground- and excited-state energy estimation.
Phys. Rev. A, 105:022417.

Cortes, C. L. and Gray, S. K. (2022b).
Quantum krylov subspace algorithms for ground-and excited-state energy estimation.
Physical Review A, 105(2):022417.

Epperly, E. N., Lin, L., and Nakatsukasa, Y. (2022).
A theory of quantum subspace diagonalization.
SIAM Journal on Matrix Analysis and Applications, 43:1263–1290.

Gilyén, A., Su, Y., Low, G. H., and Wiebe, N. (2019).
Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics.
In *Proceedings of the 51st annual ACM SIGACT symposium on theory of computing*, pages 193–204.

Grover, L. and Rudolph, T. (2002).
Creating superpositions that correspond to efficiently integrable probability distributions.
arXiv preprint quant-ph/0208112.

Hales, L. and Hallgren, S. (2000).
An improved quantum fourier transform algorithm and applications.
In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 515–525. IEEE.

Harrow, A. W., Hassidim, A., and Lloyd, S. (2009).
Quantum algorithm for linear systems of equations.
Physical Review Letters, 103(15):150502.

Jordan, S. (2011).
Quantum algorithms zoo, last updated: August 23, 2024.
https://quantumalgorithmzoo.org/.

Kirby, W., Motta, M., and Mezzacapo, A. (2023).
Exact and efficient lanczos method on a quantum computer.
Quantum, 7:1018.

Kitaev, A. Y., Shen, A., and Vyalyi, M. N. (2002).
Classical and quantum computation.
Number 47. American Mathematical Soc.

Klymko, K., Mejuto-Zaera, C., Cotton, S. J., Wudarski, F., Urbanek, M., Hait, D., Head-Gordon, M., Whaley, K. B., Moussa, J., Wiebe, N., de Jong, W. A., and Tubman, N. M. (2022).
Real-time evolution for ultracompact hamiltonian eigenstates on quantum hardware.
PRX Quantum, 3:020323.

Kothari, R. (2014).
Efficient algorithms in quantum query complexity.
PhD thesis, University of Waterloo.

Laneve, L. (2023).
Robust black-box quantum-state preparation via quantum signal processing.
arXiv preprint arXiv:2305.04705.

Li, H., Ni, H., and Ying, L. (2023).
On efficient quantum block encoding of pseudo-differential operators.
Quantum, 7:1031.

Lin, L. (2022).
Lecture notes on quantum algorithms for scientific computation.
arXiv preprint arXiv:2201.08309.

Lipton, R. J. and Regan, K. W. (2021).
Introduction to quantum algorithms via linear algebra.
MIT Press.

Liu, D., Du, W., Lin, L., Vary, J. P., and Yang, C. (2025).
An efficient quantum circuit for block encoding a pairing hamiltonian.
Journal of Computational Science, 85:102480.

Loke, T. and Wang, J. B. (2017).
Efficient quantum circuits for szegedy quantum walks.
Annals of Physics, 382:64–84.

Low, G. H. and Chuang, I. L. (2019).
Hamiltonian simulation by qubitization.
Quantum, 3:163.

Motta, M., Sun, C., Tan, A. T., ORourke, M. J., Ye, E., Minnich, A. J., Brandao, F. G., and Chan, G. K.-L. (2020).
Determining eigenstates and thermal states on a quantum computer using quantum imaginary time evolution.
Nature Physics, 16(2):205–210.

Nguyen, Q. T., Kiani, B. T., and Lloyd, S. (2022).
Block-encoding dense and full-rank kernels using hierarchical matrices: applications in quantum numerical linear algebra.
Quantum, 6:876.

Nielsen, M. A. and Chuang, I. L. (2001).
Quantum computation and quantum information, volume 2.
Cambridge University Press, Cambridge.

Parrish, R. M. and McMahon, P. L. (2019).
Quantum filter diagonalization: Quantum eigendecomposition without full quantum phase estimation.
arXiv preprint arXiv:1909.08925.

Preskill, J. (1998).
Lecture notes for physics 229: Quantum information and computation.
California Institute of Technology.

Seki, K. and Yunoki, S. (2021).
Quantum power method by a superposition of time-evolved states.
PRX Quantum, 2(1):010333.

Somma, R., Childs, A., and Kothari, R. (2016).
Quantum linear systems algorithm with exponentially improved dependence on precision.
In *APS March Meeting Abstracts*, volume 2016, pages H44–001.

Somma, R. and Subasi, Y. (2021).
Quantum state verification in the quantum linear systems problem.
In *APS March Meeting Abstracts*, volume 2021, pages R34–012.

Stair, N. H., Huang, R., and Evangelista, F. A. (2020).
A multireference quantum krylov algorithm for strongly correlated electrons.
Journal of Chemical Theory and Computation, 16:22362245.

Sünderhauf, C., Campbell, E., and Camps, J. (2024).
Block-encoding structured matrices for data input in quantum computing.
Quantum, 8:1226.

Szegedy, M. (2004).
Quantum speed-up of markov chain based algorithms.
In *45th Annual IEEE symposium on foundations of computer science*, pages 32–41. IEEE.

Wang, S., Wang, Z., Cui, G., Shi, S., Shang, R., Fan, L., Li, W., Wei, Z., and Gu, Y. (2021).
Fast black-box quantum state preparation based on linear combination of unitaries.
Quantum Information Processing, 20(8):270.

Weinstein, Y. S., Pravia, M., Fortunato, E., Lloyd, S., and Cory, D. G. (2001).
Implementation of the quantum fourier transform.
Physical review letters, 86(9):1889.

Wolf, R. D. (2019).
Quantum computing: Lecture notes.
arXiv preprint arXiv:1907.09415.

Yiğit Subaşı, R. D. S. and Orsucci, D. (2019).
Quantum algorithms for systems of linear equations inspired by adiabatic quantum computing.
Physical Review Letters, 122(6):060504.

Zhang, X.-M., Li, T., and Yuan, X. (2022).
Quantum state preparation with optimal circuit depth: Implementations and applications.
Physical Review Letters, 129(23):230504.