QUANTUM ALGORITHMS I

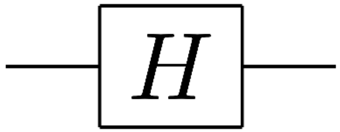
Giacomo De Palma

Quantum algorithms

- Quantum algorithm: finite sequence of elementary instructions for quantum computer
- We will consider quantum circuit model
- Elementary instructions:
  - Initialize qubit in |0>
  - Quantum gate belonging to universal set (e.g., {Hadamard, CNOT, T})
  - Measure qubit in |0>, |1> basis
- Algorithm complexity: # of elementary instructions

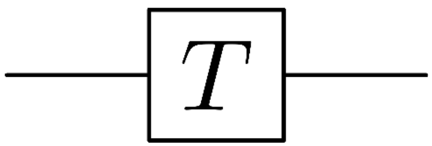
Universal set of quantum gates

- Hadamard



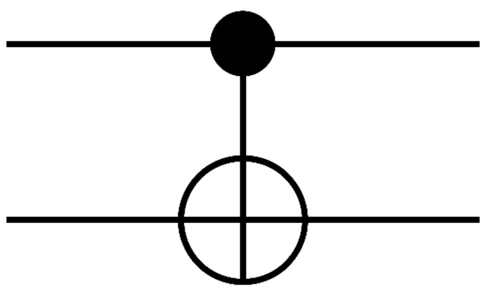
$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

- T



$$T|0\rangle = |0\rangle \qquad T|1\rangle = e^{\frac{i\pi}{4}}|1\rangle$$

- CNOT



$$CNOT|c, t\rangle = |c, t \oplus c\rangle$$

Digital quantum algorithms: overview

- Most quantum algorithms based on few primitive subroutines
- Quantum Fourier transform (exponential speedup)
  - Quantum phase estimation
    - Quantum linear algebra
    - Shor (factoring)
    - Hidden subgroup problem
- Amplitude amplification (quadratic speedup)
  - Grover search
  - Quantum counting
- Quantum singular value transform

Quantum Fourier transform

- Vectors of computational basis for *n* qubits labeled by strings of *n* bits (binary representation of natural number)

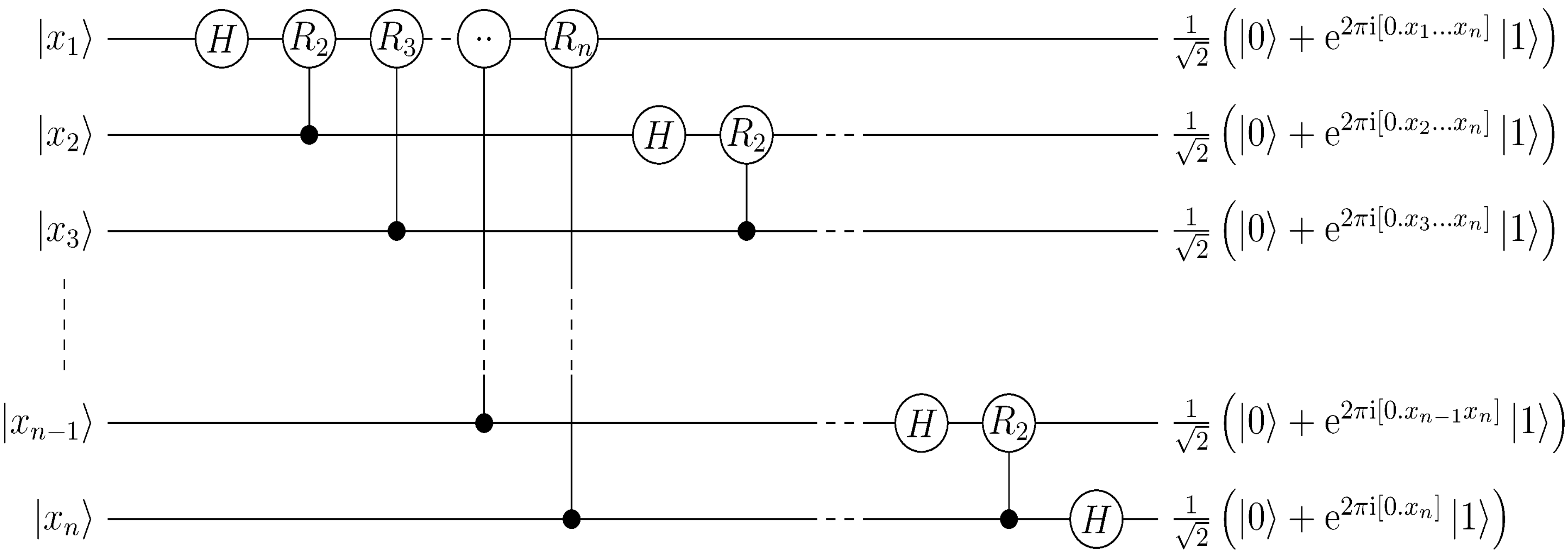
$$x \in \{0,1\}^n \sim \{0, \ldots, 2^n - 1\} \qquad |x\rangle = |x_1\rangle \otimes \ldots \otimes |x_n\rangle$$

$$\hat{f}(k) = \int_{\mathbb{R}} f(x)\, e^{ikx}\, dx$$

$$(QFT\psi)(y) = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} \psi(x) \qquad y \in \{0,1\}^n$$

$$QFT|x\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle = \bigotimes_{k=1}^{n} \frac{|0\rangle + e^{\frac{2\pi i x}{2^k}} |1\rangle}{\sqrt{2}}$$

QFT circuit



$$R_k|0\rangle = |0\rangle \qquad R_k|1\rangle = e^{\frac{2\pi i}{2^k}}|1\rangle$$

- Requires $\Theta(n^2)$ gates

Quantum phase estimation

- We can apply unknown U on m qubits as black box; we have eigenstate $|u>$ with unknown eigenvalue $e^{2\pi i\varphi}$
  Problem: find φ
- Algorithm: let V act on $n + m$ qubits as

$$V|x\rangle|\psi\rangle = |x\rangle \otimes U^x|\psi\rangle \qquad x \in \{0,1\}^n$$

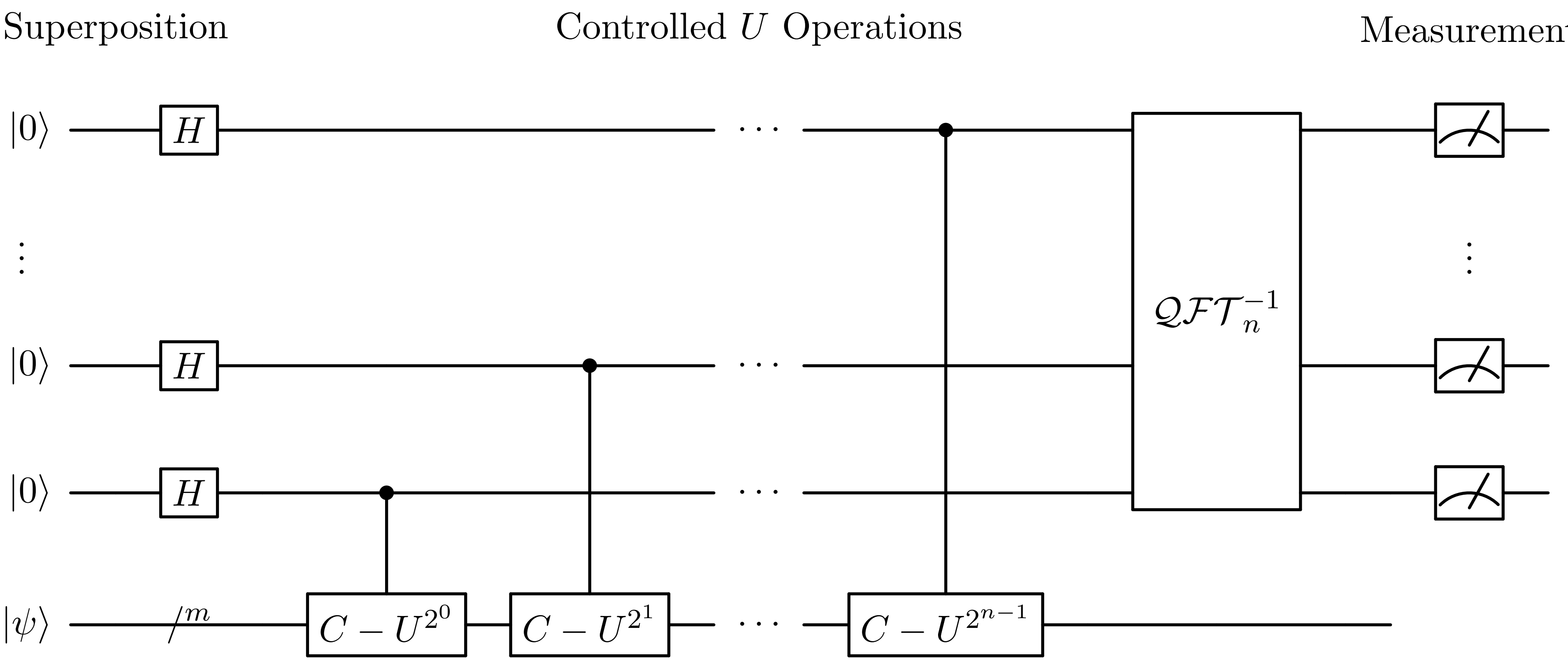
- Build the state

$$V\left(\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}|x\rangle\right)|u\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}e^{2\pi i\varphi x}|x\rangle|u\rangle$$

$$\approx QFT|2^n\varphi\rangle \otimes |u\rangle$$

- Apply inverse QFT, measure first n qubits, read (n-bit estimate of) φ

QPE circuit



- Requires $\Theta(n^2)$ gates + 1 call to $U^{2^\wedge k}$, $k < n$

HHL

- Problem: Given *m*-qubit sparse Hamiltonian *H* (each row has *O*(1) nonzero elements) and state |*ψ*>, build $H^{-1}|\psi>$

- Let $$H = \sum_k \lambda_k |u_k\rangle\langle u_k| \qquad |\psi\rangle = \sum_k \psi_k |u_k\rangle$$

- Apply QPE to $U = e^{2\pi iH}$ and |*ψ*> (needs Hamiltonian simulation), get

$$\sum_k \psi_k |\lambda_k\rangle |u_k\rangle$$

HHL

- Add qubit in |0>, apply rotation

$$|\lambda_k\rangle|0\rangle \mapsto |\lambda_k\rangle \left(\sqrt{1 - \frac{1}{\|H^{-1}\|^2 \lambda_k^2}} \, |0\rangle + \frac{1}{\|H^{-1}\| \lambda_k} \, |1\rangle \right)$$

- Get

$$\sum_k \psi_k \, |\lambda_k\rangle|u_k\rangle \left(\sqrt{1 - \frac{1}{\|H^{-1}\|^2 \lambda_k^2}} \, |0\rangle + \frac{1}{\|H^{-1}\| \lambda_k} \, |1\rangle \right)$$

- Measure auxiliary qubit and postselect on outcome 1, get

$$\sum_k \frac{\psi_k}{\|H^{-1}\| \lambda_k} |\lambda_k\rangle|u_k\rangle|1\rangle$$

HHL

- Apply inverse QPE and discard ancilla, get

$$\sum_k \frac{\psi_k}{\|H^{-1}\|\,\lambda_k}|u_k\rangle = \sum_k \psi_k \frac{H^{-1}}{\|H^{-1}\|}|u_k\rangle = \frac{H^{-1}}{\|H^{-1}\|}|\psi\rangle$$

- Success probability $\frac{\left\|H^{-1}|\psi\rangle\right\|^2}{\|H^{-1}\|^2} \geq \frac{1}{\|H\|^2\,\|H^{-1}\|^2} = \frac{1}{\kappa^2}$
- Condition number $\kappa = \frac{\max_i |\lambda_i|}{\min_i |\lambda_i|}$
- Success probability increased to $\frac{1}{\kappa}$ by amplitude amplification
- Repeat until success
- Runtime $O\left(\frac{\kappa^2 n}{\epsilon}\right)$

HHL

- Exponential speedup for linear systems of equations!
- Caveats: preparation of initial state $|\psi>$, readout of the result $H^{-1}|\psi>$
- Can handle non-Hermitian H with extra auxiliary qubit
- Can produce $f(H)|\psi>$ for generic f

Aram W. Harrow, Avinatan Hassidim, Seth Lloyd
Quantum Algorithm for Linear Systems of Equations
Phys. Rev. Lett. 103, 150502 (2009)

Linear differential equations

- Linear ODE in $\mathbb{R}^N$, $N \gg 1$

$$\frac{dx}{dt} = Ax + b \qquad A \text{ } s\text{-sparse} \qquad 0 \le t \le T$$

- Unitary evolution if A antihermitian and $b=0$
- Eigenvalues of A with negative real part
- Discretization with $\Delta t = 1 / \|A\|$, $K = T / \Delta t$ steps
- Quantum history state

$$|\Psi\rangle = \sum_{i=0}^{K} |x_{i\Delta t}\rangle |i\rangle$$

Linear differential equations

- Euler forward method: Discretized ODE

$$x_0 = \bar{x} \qquad \frac{x_{i\Delta t} - x_{(i-1)\Delta t}}{\Delta t} = A\,x_{(i-1)\Delta t} + b$$

equivalent to linear constraint on |Ψ>

$$\mathcal{M} = \mathbb{I}_N \otimes \mathbb{I}_{K+1} - \sum_{i=1}^{K} (\mathbb{I}_N + \Delta t\, A) \otimes |i\rangle\langle i-1|$$

$$\mathcal{M}|\Psi\rangle = |x_0\rangle|0\rangle + \sum_{i=1}^{K} \left(|x_{i\Delta t}\rangle - (\mathbb{I}_N + \Delta t\, A)\,|x_{(i-1)\Delta t}\rangle\right)|i\rangle$$

$$= |\bar{x}\rangle|0\rangle + \Delta t|b\rangle \sum_{i=1}^{K} |i\rangle$$

Linear differential equations

- Apply HHL to generate history state

$$|\Psi\rangle = \mathcal{M}^{-1}\left(|\bar{x}\rangle|0\rangle + \Delta t|b\rangle\sum_{i=1}^{K}|i\rangle\right)$$

- Measure history state to extract information on the solution (getting the whole solution has complexity $\Omega(N)$)

- Algorithm improved to complexity

$$\tilde{O}\left(\kappa T \|A\| s\right) \qquad \kappa = \|V\|\left\|V^{-1}\right\| : A = V D V^{-1}$$

Dominic W. Berry, Andrew M. Childs, Aaron Ostrander, Guoming Wang
Quantum Algorithm for Linear Differential Equations with Exponentially Improved Dependence on Precision
Commun. Math. Phys. **356**, 1057 (2017)

Block encoding

- Quantum eigenvalue transform: Given $|\psi\rangle$, produce $f(H)|\psi\rangle$ where f is even or odd
- U on $\mathbb{C}^2 \otimes \mathbb{C}^N$ is a block encoding of H on $\mathbb{C}^N$ if

$$H = \langle 0|U|0\rangle \qquad U = \begin{pmatrix} H & \cdot \\ \cdot & \cdot \end{pmatrix}$$

- Requires $\|H\| \leq 1$

- Quantum eigenvalue transform generates block encoding of $f(H)$

$$f(H) = \langle 0|\tilde{U}|0\rangle \qquad \tilde{U} = \begin{pmatrix} f(H) & \cdot \\ \cdot & \cdot \end{pmatrix}$$

Block encoding

- Diagonalize *H*

$$H = \sum_\lambda \lambda \left|\lambda\right\rangle\left\langle\lambda\right| \qquad -1 \leq \lambda \leq 1$$

- Simplified explicit block encoding

$$U = \begin{pmatrix} H & i\sqrt{\mathbb{I} - H^2} \\ i\sqrt{\mathbb{I} - H^2} & H \end{pmatrix} = \sum_\lambda U_\lambda \otimes \left|\lambda\right\rangle\left\langle\lambda\right|$$

$$U_\lambda = \begin{pmatrix} \lambda & i\sqrt{1 - \lambda^2} \\ i\sqrt{1 - \lambda^2} & \lambda \end{pmatrix}$$

Quantum signal processing

- Quantum signal processing

$$\tilde{U}_{\vec{\phi}} = e^{i\phi_1 Z} U^\dagger e^{i\phi_2 Z} U \ldots e^{i\phi_{2d-1} Z} U^\dagger e^{i\phi_{2d} Z} U$$

$$= \sum_\lambda e^{i\phi_1 Z} U_\lambda^\dagger e^{i\phi_2 Z} U_\lambda \ldots e^{i\phi_{2d} Z} U_\lambda \otimes |\lambda\rangle\langle\lambda|$$

$$= \sum_\lambda \begin{pmatrix} P(\lambda) & i\,Q(\lambda)\sqrt{1-\lambda^2} \\ i\,Q(\lambda)^*\sqrt{1-\lambda^2} & P(\lambda)^* \end{pmatrix} \otimes |\lambda\rangle\langle\lambda|$$

- deg $P \leq 2d$; deg $Q \leq 2d - 1$
- P even; Q odd
- $|P(\lambda)|^2 + (1-\lambda^2)\,|Q(\lambda)|^2 = 1$

Quantum eigenvalue transform

- For any *P*, *Q* as before there exists $\vec{\phi}$ such that $U_{\vec{\phi}}$ is a block encoding of *P*(*H*)
- With auxiliary qubit we can get rid of constraint on the existence of *Q*: Let *U* be a block encoding of *H*, and let *P* be a polynomial of degree *d* with parity *d* mod 2 such that

$$|P(\lambda)| \leq 1 \qquad \forall\, \lambda \in [-1, 1]$$

- Then, a block encoding of *P*(*H*) can be realized with *d* applications of *U* / $U^\dagger$ and *d* phase shifts in the *Z* basis

Application to linear systems of equations

- Let *H* be such that $\frac{\mathbb{I}}{\kappa} \leq |H| \leq \mathbb{I}$
- Let *P*(*λ*) be a polynomial approximation of $\frac{1}{\kappa\,\lambda}$ for $\frac{1}{\kappa} \leq |\lambda| \leq 1$
- Let *U* be a block encoding of *H* and let $\tilde{U}$ be a block encoding of *P*(*H*)
- We have

$$\tilde{U}|0\rangle|\psi\rangle = \begin{pmatrix} P(H) & \cdot \\ \cdot & \cdot \end{pmatrix} \begin{pmatrix} |\psi\rangle \\ 0 \end{pmatrix}$$

$$= |0\rangle \otimes P(H)|\psi\rangle + |1\rangle \otimes |\mathrm{garbage}\rangle$$

Application to linear systems of equations

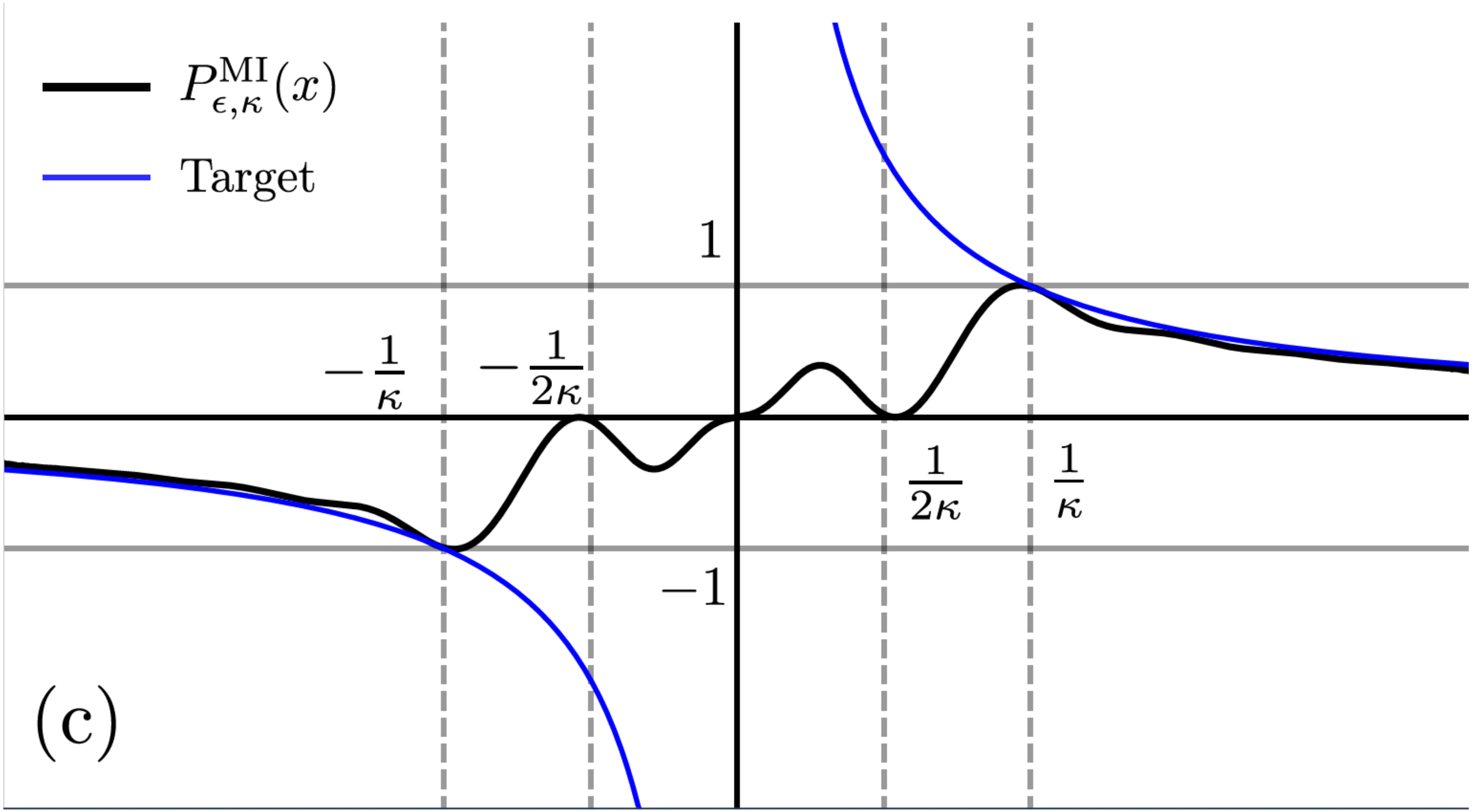
- Measure auxiliary qubit and condition on 0. Get

  $$P(H)|\psi\rangle \simeq \frac{H^{-1}}{\kappa}|\psi\rangle$$ with probability at least $\frac{1}{\kappa^2}$

  increased to $\frac{1}{\kappa}$ by amplitude amplification
- There exists an odd *P*(*λ*) approximating $\frac{1}{\kappa\,\lambda}$ for $\frac{1}{\kappa} \leq |\lambda| \leq 1$

  with precision $\frac{\epsilon}{\kappa}$ and degree $O\left(\kappa \log \frac{\kappa}{\epsilon}\right)$
- The algorithm requires $O\left(\kappa^2 \log \frac{\kappa}{\epsilon}\right)$ calls to *U*
- Dependence on size of *H* hidden in cost of *U*

Matrix inversion polynomial



Finding block encodings

- Let *A* be a *O*(1) sparse matrix on *n* qubits (each row and each column have *O*(1) nonzero elements) whose nonzero entries have absolute value at most 1. Then, there exists an approximate block-encoding of *A* requiring $O\left(n + \log^{2.5}\frac{1}{\epsilon}\right)$ elementary gates and *O*(1) uses of oracles for the nonzero entries of *A*

QSVT References

- Tutorial: John M. Martyn, Zane M. Rossi, Andrew K. Tan, Isaac L. Chuang, “Grand Unification of Quantum Algorithms”, PRX Quantum 2, 040203 (2021)
- Technical paper: András Gilyén, Yuan Su, Guang Hao Low, Nathan Wiebe, “Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics”, arXiv:1806.01838