The quantum query complexity of implementing black-box unitary transformations

Dominic Berry
IQC, Waterloo

Andrew Childs
C&O and IQC, Waterloo

arXiv:0910.4157 [quant-ph]

Implementing unitaries

Suppose we want to implement a general $N \times N$ unitary operation.

How many elementary operations are required?

Simple counting arguments: $\Omega(N^2)$ gates just to approximate a general unitary with fixed precision.

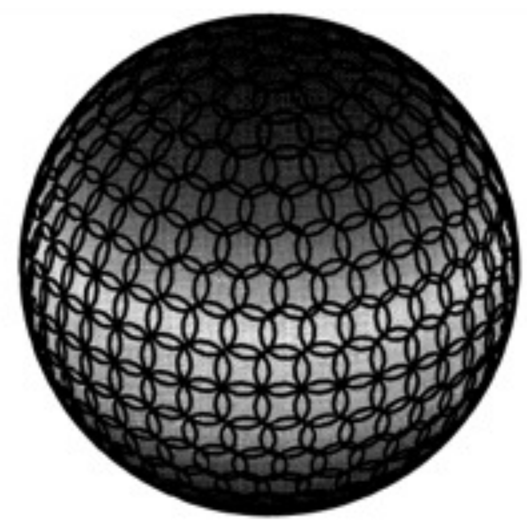


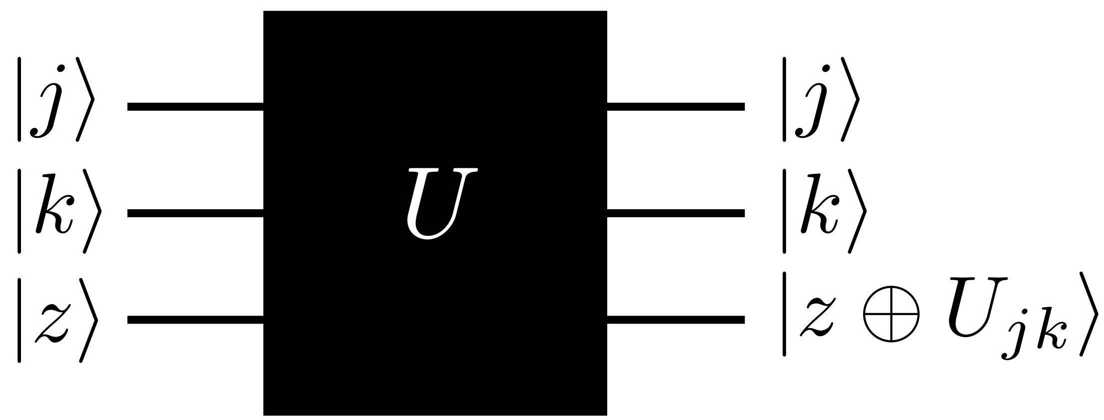
Figure 4.18. Visualization of covering the set of possible states with patches of constant radius.

Any unitary can be decomposed into $N^2\ \mathrm{poly}(\log N)$ two-level unitary matrices, so this is nearly achievable.

$$\begin{pmatrix}
1 & & & & & & & & & & \\
 & \ddots & & & & & & & & & \\
 & & 1 & & & & & & & & \\
 & & & a & & & & b & & & \\
 & & & & 1 & & & & & & \\
 & & & & & \ddots & & & & & \\
 & & & & & & 1 & & & & \\
 & & & c & & & & d & & & \\
 & & & & & & & & 1 & & \\
 & & & & & & & & & \ddots & \\
 & & & & & & & & & & 1
\end{pmatrix}$$

Black-box unitaries

Another scenario: the matrix elements of U are provided by a black box.



This models the setting where we can efficiently compute the matrix elements.

Counting arguments no longer apply!

What we know: To implement U with bounded error,

$\Omega(\sqrt{N})$ queries are necessary

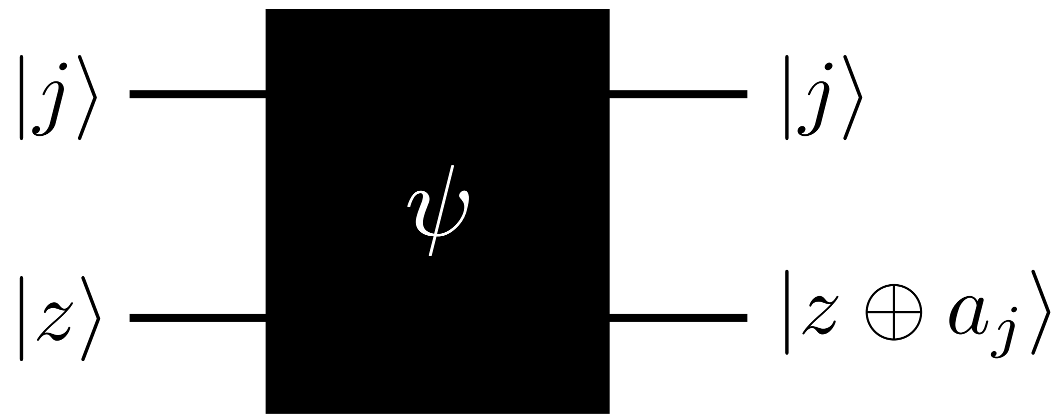
$O(N^{2/3}(\log\log N)^{4/3})$ queries are sufficient

Outline

1. Black-box state preparation
2. Lower bound for black-box unitaries
3. Implementing unitaries by Hamiltonian simulation: $N^{3/4}$
4. Examples
5. Improved implementation by breaking up the Hamiltonian: $N^{2/3}$
6. Summary and open questions

Black box state preparation

Related problem: prepare a state $|\psi\rangle = \sum_{j=1}^{N} a_j |j\rangle$ given a black box for its amplitudes.



In general, $\Omega(\sqrt{N})$ queries are required (search).

Grover 2000: $O(\sqrt{N})$ queries are sufficient!

State preparation by amplitude amplification

Start from $\frac{1}{\sqrt{N}}\sum_{j=1}^{N}|j\rangle$

With two queries, we can prepare

$$|\phi\rangle := \frac{1}{\sqrt{N}}\sum_{j=1}^{N}\left(a_j|j,0\rangle + \sqrt{1-|a_j|^2}\,|j,1\rangle\right)$$

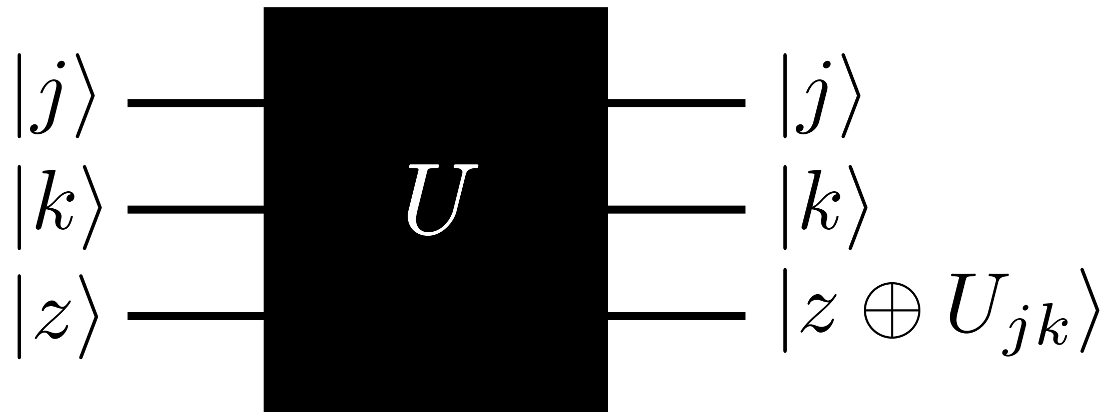
Amplitude amplification: Alternately reflect about $|\phi\rangle$ and the subspace with $|0\rangle$ in the second register. Rotate in the two-dimensional subspace $\mathrm{span}\{|\psi\rangle, |\phi\rangle\}$ where

$$|\psi\rangle := \sum_j a_j|j,0\rangle$$

Time to prepare $|\psi\rangle$: $\frac{1}{|\langle\psi|\phi\rangle|} = \frac{\sqrt{N}}{\sum_{j=1}^{N}|a_j|^2} = \sqrt{N}$

Grover 2000

Black-box unitaries: Lower bound



Search with a unique marked item:
Given a binary string $x_1 x_2 \ldots x_N$ with exactly one $x_i = 1$, find i.

Consider $U_{jk} = x_{j-k \bmod N}$.

Black box for x → black box for U.

Since $U|0\rangle = |i\rangle$, implementing U performs the search.

So implementing U requires $\Omega(\sqrt{N})$ queries, by BBBV 1997.

Note: This bound cannot be improved using permutation matrices.

From Hamiltonians to unitaries

To implement U, simulate the Hamiltonian $H = \begin{pmatrix} 0 & U \\ U^\dagger & 0 \end{pmatrix}$.

Since $H^2 = I$, we have $e^{-\mathrm{i}Ht} = \cos(t)I - \mathrm{i}\sin(t)H$.

So simulating H for time $\pi/2$ implements U:

$$e^{-\mathrm{i}H\pi/2}|1\rangle \otimes |\psi\rangle = -\mathrm{i}|0\rangle \otimes U|\psi\rangle$$

Hamiltonian simulation by quantum walk

One way to simulate H is to implement a related discrete-time (Szegedy) quantum walk.

Expand space from $\mathbb{C}^N$ to $\mathbb{C}^{N+1} \otimes \mathbb{C}^{N+1}$.

Alternately swap the two registers and reflect about $\operatorname{span}\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$, where

$$|\psi_j\rangle := |j\rangle \otimes \left(\frac{1}{\sqrt{\|H\|_1}} \sum_{k=1}^{N} \sqrt{H_{jk}^*}\, |k\rangle + \nu_j |N+1\rangle \right)$$

$$\|H\|_1 := \max_j \textstyle\sum_{k=1}^{N} |H_{jk}|$$

Using phase estimation, $O(\|Ht\|_1/\delta)$ steps of this walk suffice to simulate H for time t with error at most δ (in trace distance).

AMC, arXiv:0810.0312, to appear in Commun. Math. Phys.

Application to black-box unitaries

Simulate $H = \begin{pmatrix} 0 & U \\ U^\dagger & 0 \end{pmatrix}$ for $t = \pi/2$.

We have $\|H\|_1 = \|U\|_1 \le \sqrt{N}$, so $O(\sqrt{N})$ steps of the walk suffice.

To implement the walk, note that reflection about $|\psi\rangle$ reduces to preparing $|\psi\rangle$: given a circuit performing $|0\rangle \overset{V}{\mapsto} |\psi\rangle$,

$$
\begin{aligned}
|\psi\rangle &\overset{V^\dagger}{\mapsto} |0\rangle & \qquad |\psi^\perp\rangle &\overset{V^\dagger}{\mapsto} |0^\perp\rangle \\
&\mapsto -|0\rangle & &\mapsto |0^\perp\rangle \\
&\overset{V}{\mapsto} -|\psi\rangle & &\overset{V}{\mapsto} |\psi^\perp\rangle
\end{aligned}
$$

State preparation in $O(\sqrt{N})$ queries [Grover 2000]
$\Rightarrow$ Implementation of U in $O(N)$ queries.

State preparation revisited

Prepare $\sum_{j=1}^{N} a_j|j\rangle$ with the assumption that $|a_j| \le A$.

With two queries, we can prepare

$$|\phi\rangle := \frac{1}{\sqrt{N}} \sum_{j=1}^{N} \left(\frac{a_j}{A}|j,0\rangle + \sqrt{1 - \frac{|a_j|^2}{A^2}}\,|j,1\rangle \right)$$

Amplitude amplification: Alternately reflect about $|\phi\rangle$ and the subspace with $|0\rangle$ in the second register. Rotate in the two-dimensional subspace $\mathrm{span}\{|\psi\rangle, |\phi\rangle\}$ where

$$|\psi\rangle := \sum_j a_j|j,0\rangle$$

Time to prepare $|\psi\rangle$: $\dfrac{1}{|\langle\psi|\phi\rangle|} = \dfrac{\sqrt{N}A}{\sum_{j=1}^{N}|a_j|^2} = \sqrt{N}A$

Tradeoff

The simulation is slow because when $\|H\|_1 \gg 1$, each step of the quantum walk doesn't do much:

$$|\psi_j\rangle := |j\rangle \otimes \left(\frac{1}{\sqrt{\|H\|_1}} \sum_{k=1}^{N} \sqrt{H^*_{jk}}\, |k\rangle + \nu_j |N+1\rangle \right)$$

is close to $|N+1\rangle$.

But consequently, $|\psi_j\rangle$ is easier to prepare!

States with amplitudes at most A: black-box state preparation in $O(\sqrt{N}A)$ queries.

Result: Implementation of a black-box U with query complexity

$$O\left(\sqrt{N\|U\|_1 \max(U)}\right)$$

Worst case: $\|U\|_1 \leq \sqrt{N}$ and $\max(U) \leq 1$, giving $O(N^{3/4})$ queries.

Examples: Permutations, Fourier transforms

General query complexity: $O\left(\sqrt{N\|U\|_1 \max(U)}\right)$

If U is a permutation, $\|U\|_1 = 1$ and $\max(U) = 1$.
Query complexity is $O(\sqrt{N})$.

If U is the discrete Fourier transform, $\|U\|_1 = \sqrt{N}$ and $\max(U) = 1/\sqrt{N}$.
Query complexity is $O(\sqrt{N})$.

Hard cases have a mix of small and large entries.

Examples: Rotation of a big spin

General query complexity: $O\left(\sqrt{N\|U\|_1 \max(U)}\right)$

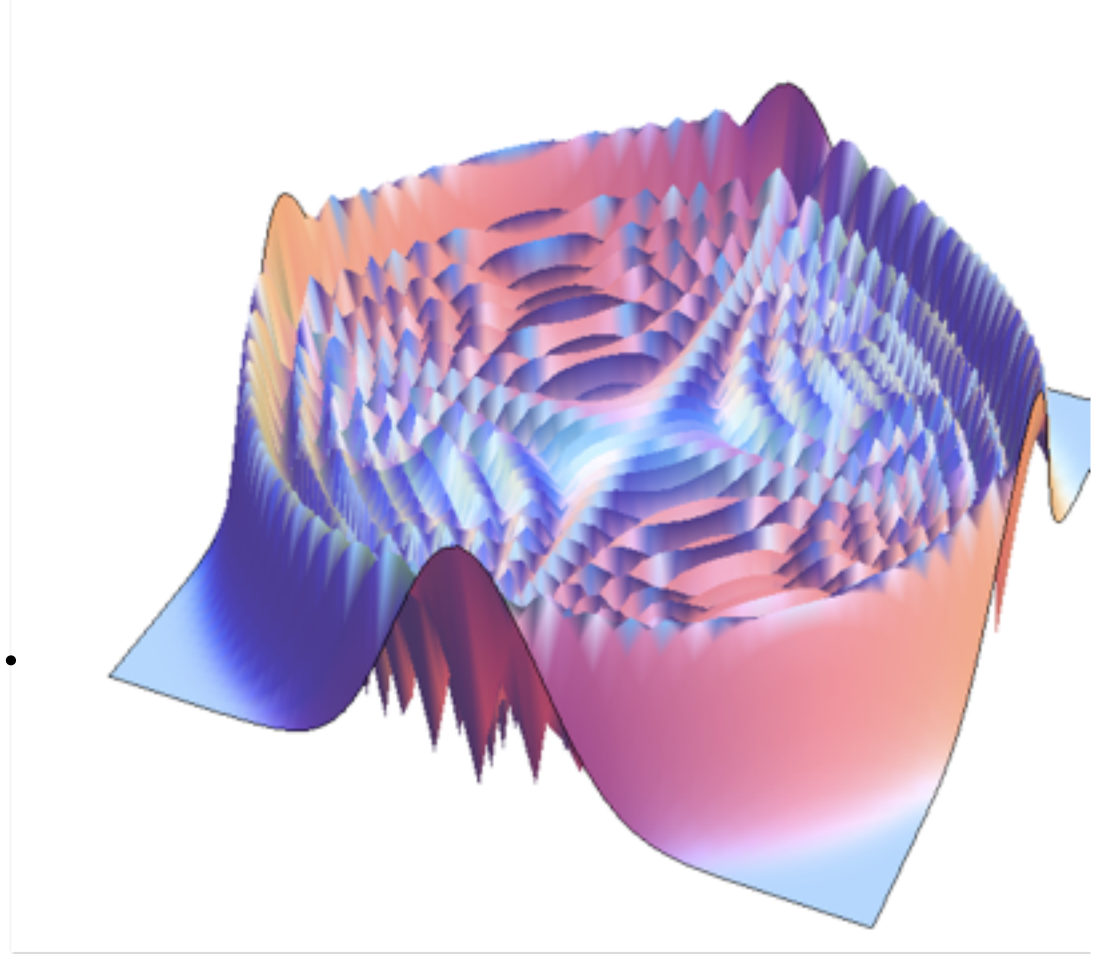
Consider a spin-J particle (dimension $2J+1$).

Let $U = e^{-i\pi J_x/2}$ (in J_z basis).

Then $\|U\|_1 = O(\sqrt{J})$ and

$$\max(U) = O(J^{-1/4})$$

So the algorithm uses $O(J^{5/8})$ queries.



Controlling error: Lazy quantum walk

To keep the error under control, we actually define the walk with

$$|\psi_j^\epsilon\rangle := |j\rangle \otimes \left(\sqrt{\frac{\epsilon}{\|H\|_1}} \sum_{k=1}^{N} \sqrt{H_{jk}^*}\, |k\rangle + \nu_j \sqrt{1-\epsilon}\, |N+1\rangle \right)$$

Number of queries used in a simulation for time t:

$$O\left(t \sqrt{\frac{N\|H\|_1 \max(H)}{\epsilon}} \right)$$

Error in amplitude amplification: $O(\|Ht\|\epsilon)$

For total error at most δ, number of queries required:

$$O\left(t^{3/2} \sqrt{\frac{N\|H\|_1 \max(H)\|H\|}{\delta}} \right)$$

Breaking up the Hamiltonian

Hard cases have a mix of small and large entries.

Strategy: Write $H = \sum_{\ell=1}^{L} H_\ell$ such that all nonzero entries of H_ℓ have similar magnitudes.

Recombine using Lie-Trotter-Suzuki formulae:

$$\begin{aligned}
\left(e^{-\mathrm{i}At/n}e^{-\mathrm{i}Bt/n}\right)^n &\approx e^{-\mathrm{i}(A+B)t} \\
\left(e^{-\mathrm{i}At/2n}e^{-\mathrm{i}Bt/n}e^{-\mathrm{i}At/2n}\right)^n &\approx e^{-\mathrm{i}(A+B)t} \\
&\vdots
\end{aligned}$$

Breaking up the Hamiltonian: Best case, 2 terms

General query complexity: $O\left(\sqrt{N\|H\|_1 \max(H)\|H\|}\right)$

Write $H = H_{\text{small}} + H_{\text{big}}$ with

- $\max(H_{\text{small}}) \le h$
- every nonzero entry of H_{big} of magnitude at least h

Then we have

$\|H_{\text{small}}\|_1 \le \sqrt{N}$ ⇒ query complexity $O(N^{3/4}\sqrt{h})$ for H_{small}

$\|H_{\text{big}}\|_1 \le \max_j \sum_{k=1}^n \frac{|(H_{\text{big}})_{jk}|^2}{h} \le \frac{1}{h}$ and $\max(H_{\text{big}}) \le 1$

⇒ query complexity $O(\sqrt{N/h})$ for H_{big}

With $h = N^{-1/4}$, assuming $\|H_{\text{small}}\|, \|H_{\text{big}}\| = O(\|H\|) = O(1)$, overall query complexity is $O(N^{5/8})$.

Breaking up the Hamiltonian: Best case

Strategy: Write $H = \sum_{\ell=1}^{L} H_\ell$ such that all nonzero entries of H_ℓ have similar magnitudes.

General query complexity: $O\left(\sqrt{N\|H\|_1 \max(H)\|H\|}\right)$

Suppose the nonzero entries satisfy $h_\ell \le |(H_\ell)_{jk}| \le h_{\ell-1}$.

Then $\max(H_\ell) \le h_{\ell-1}$ and $\|H_\ell\|_1 \le 1/h_\ell$

$\Rightarrow$ query complexity $O(\sqrt{N h_{\ell-1}/h_\ell})$ for H_ℓ.

Taking $h_\ell \approx h_{\ell-1}$ for all ℓ, and with all $\|H_\ell\| = O(1)$, overall query complexity is $O(\sqrt{N})$.

Careful error analysis, assuming all $\|H_\ell\| = O(1)$: $\sqrt{N}\,\mathrm{poly}(\log N)$

But this assumption does not hold in general!

Breaking up the Hamiltonian: Worst case

Strategy: Write $H = \sum_{\ell=1}^{L} H_\ell$ such that all nonzero entries of H_ℓ have similar magnitudes.

General query complexity: $O\left(\sqrt{N\|H\|_1 \max(H)\|H\|}\right)$

Suppose the nonzero entries satisfy $h_\ell \le |(H_\ell)_{jk}| \le h_{\ell-1}$.

Then $\|H_\ell\| \le \|H_\ell\|_1 \le \|H\|^2/h_\ell = 1/h_\ell$.
So simulating H_ℓ takes $O(\sqrt{N/h_\ell})$ queries, assuming $h_\ell \approx h_{\ell-1}$.

With very small entries, can simulate without amplitude amplification:
Simulating H_L takes $O(N h_{L-1})$ queries.

Set $N h_{L-1} = \sqrt{N/h_{L-1}}$: take $h_{L-1} \approx N^{-1/3}$ to get $O(N^{2/3})$.

Careful error analysis: $O(N^{2/3}(\log\log N)^{4/3})$

Summary

To implement U with bounded error,

$$\Omega(\sqrt{N}) \text{ queries are necessary}$$
$$O(N^{2/3}(\log\log N)^{4/3}) \text{ queries are sufficient}$$

(Dependence on error is also understood.)

Open questions

- Is black-box state preparation asymptotically easier than implementing a black-box unitary?
  - Improve the lower bound?
  - Improve the algorithm?
- Applications to quantum algorithms?