CS 498QC Final Project - Literature Review

“On the Hardness of Detecting Macroscopic Superpositions” by Scott Aaronson, Yosi Atia and Leonard Susskind

Wenqi He (wenqihe2)

November 27, 2023

Superposition and Mixture

Definition

Equal superpositions $|\psi\rangle$ and $|\phi\rangle$ of orthogonal states $|x\rangle$ and $|y\rangle$:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|y\rangle\,, \quad |\phi\rangle = \frac{1}{\sqrt{2}}|x\rangle - \frac{1}{\sqrt{2}}|y\rangle$$

$$|x\rangle = \frac{1}{\sqrt{2}}|\psi\rangle + \frac{1}{\sqrt{2}}|\phi\rangle\,, \quad |y\rangle = \frac{1}{\sqrt{2}}|\psi\rangle - \frac{1}{\sqrt{2}}|\phi\rangle$$

Definition

An *equal mixture* of $|x\rangle$ and $|y\rangle$, or equivalently, $|\psi\rangle$ and $|\phi\rangle$:

$$\rho_{mixed} = \frac{1}{2}|x\rangle\langle x| + \frac{1}{2}|y\rangle\langle y| = \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|$$

Distinguishing

Definition

A **distinguisher** for $|\psi\rangle$ and $|\phi\rangle$ with bias Δ is a circuit U that accepts $|\psi\rangle$ with probability p and $|\phi\rangle$ with probability $p - \Delta$.

Specifically, we measure the first qubit after applying U and accept the state if the outcome is $|0\rangle$.

$$\langle 0| \operatorname{tr}_{aux}\left(U|\psi\rangle\langle\psi|U^\dagger\right)|0\rangle = p$$

$$\langle 0| \operatorname{tr}_{aux}\left(U|\phi\rangle\langle\phi|U^\dagger\right)|0\rangle = p - \Delta$$

Distinguishing

Lemma

A distinguisher U for $|\psi\rangle$ and $|\phi\rangle$ also distinguishes them from an equal mixture of $|x\rangle$ and $|y\rangle$ with bias $\Delta/2$.

Proof:

$$
\begin{aligned}
&\langle 0| \operatorname{tr}_{aux}\left(U\rho_{mixed}U^{\dagger}\right)|0\rangle \\
&= \langle 0| \operatorname{tr}_{aux}\left(U\left(\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|\right)U^{\dagger}\right)|0\rangle \\
&= \frac{1}{2}\langle 0| \operatorname{tr}_{aux}\left(U|\psi\rangle\langle\psi|U^{\dagger}\right)|0\rangle + \frac{1}{2}\langle 0| \operatorname{tr}_{aux}\left(U|\phi\rangle\langle\phi|U^{\dagger}\right)|0\rangle \\
&= \frac{|a|^2 + |c|^2}{2} = p - \frac{\Delta}{2}
\end{aligned}
$$

$\square$

Swapping

Definition

A **swapper** of $|x\rangle$ and $|y\rangle$ with error ε is a unitary U that satisfies

$$\text{“fidelity” of } U := \frac{|\langle y| U |x\rangle + \langle x| U |y\rangle|}{2} = 1 - \varepsilon.$$

When $\varepsilon = 0$, either U or $-U$ is a perfect swapper.

Definition

The **swap complexity** $\mathcal{S}_\varepsilon(|x\rangle, |y\rangle)$ is the minimum number of gates needed for a swapper of $|x\rangle$ and $|y\rangle$ with error at most ε.

The Hardness of Detecting (Macroscopic) Superpositions

Theorem (Distinguishability $\leftrightarrow$ Swappability)

The circuit complexity of distinguishing $|\psi\rangle$ and $|\phi\rangle$ from an equal mixture of $|x\rangle$ and $|y\rangle$ with bias Δ is the same as the circuit complexity of swapping $|x\rangle$ and $|y\rangle$ with fidelity 2Δ, i.e., $\mathcal{S}_{1-2\Delta}(|x\rangle, |y\rangle)$.

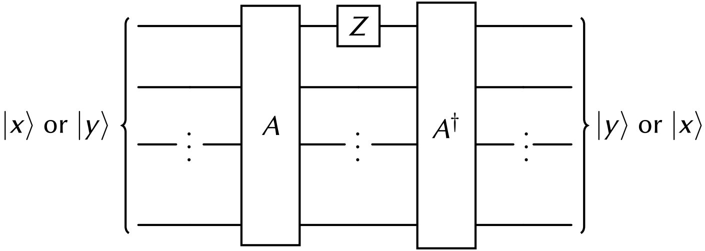
Corollary

When building an effective swapper for two orthogonal macroscopic states $|x\rangle$ and $|y\rangle$ is infeasible, it would also be infeasible to distinguish an equal superposition of $|x\rangle$ and $|y\rangle$ from an equal mixture of $|x\rangle$ and $|y\rangle$, which means it's technologically impossible to prepare or even observe such superpositions.

Distinguishability → Swappability

Theorem

If we can construct a distinguisher A for $|\psi\rangle$ and $|\phi\rangle$ with bias Δ, then with black-box access to A and $A^\dagger$ and one additional gate, we can construct a swapper for $|x\rangle$ and $|y\rangle$ with fidelity Δ.



Distinguishability $\to$ Swappability: Perfect Case

Suppose we have a perfect distinguisher A:

$$A|\psi\rangle = |0\rangle|g_0(\psi)\rangle, \quad A|\phi\rangle = |1\rangle|h_1(\phi)\rangle$$

Then

$$A|x\rangle = A\left(\frac{|\psi\rangle + |\phi\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|0\rangle|g_0(\psi)\rangle + |1\rangle|h_1(\phi)\rangle)$$
$$A|y\rangle = A\left(\frac{|\psi\rangle - |\phi\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|0\rangle|g_0(\psi)\rangle - |1\rangle|h_1(\phi)\rangle)$$
$$Z_0A|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle|g_0(\psi)\rangle - |1\rangle|h_1(\phi)\rangle) = A|y\rangle$$
$$Z_0A|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle|g_0(\psi)\rangle + |1\rangle|h_1(\phi)\rangle) = A|x\rangle$$

Circuit $U = A^\dagger Z_0 A$ is a perfect swapper:

$$U|x\rangle = A^\dagger Z_0 A|x\rangle = |y\rangle, \quad U|y\rangle = A^\dagger Z_0 A|y\rangle = |x\rangle.$$

Distinguishability $\rightarrow$ Swappability

Proof: Suppose we have a distinguisher A for $|\psi\rangle$ and $|\phi\rangle$, such that

$$A|\psi\rangle = a|0\rangle|g_0(\psi)\rangle + b|1\rangle|g_1(\psi)\rangle$$
$$A|\phi\rangle = c|0\rangle|h_0(\phi)\rangle + d|1\rangle|h_1(\phi)\rangle$$

where

$$|a|^2 = p, \quad |c|^2 = p - \Delta,$$

then

$$\langle y| U |x\rangle = \langle y| A^\dagger Z_0 A |x\rangle = -\Delta + \frac{1}{2}\left[ac\left(C_0 - C_0^*\right) + bd\left(C_1 - C_1^*\right)\right]$$
$$\langle x| U |y\rangle = \langle x| A^\dagger Z_0 A |y\rangle = -\Delta + \frac{1}{2}\left[ac\left(C_0^* - C_0\right) + bd\left(C_1^* - C_1\right)\right]$$

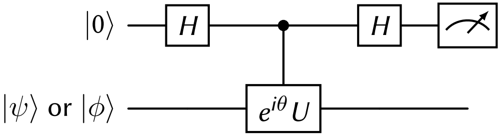
$$\frac{|\langle y| U |x\rangle + \langle x| U |y\rangle|}{2} = \Delta$$

$\square$

Swappability → Distinguishability

Theorem

If we can construct a swapper for $|x\rangle$ and $|y\rangle$ with fidelity Δ, then with black-box access to a controlled $e^{i\theta}U$ gate and two additional gates, we can construct a distinguisher for $|\psi\rangle$ and $|\phi\rangle$ with bias Δ.



Swappability $\rightarrow$ Distinguishability: Perfect Case ($\theta = 0$)

If the input state is $|\psi\rangle$: Before controlled U, the state is

$$|+\rangle|\psi\rangle = \frac{1}{2}\left(|0\rangle|x\rangle + |0\rangle|y\rangle + |1\rangle|x\rangle + |1\rangle|y\rangle\right)$$

After controlled U, the state is

$$\frac{1}{2}\left(|0\rangle|x\rangle + |0\rangle|y\rangle + |1\rangle|y\rangle + |1\rangle|x\rangle\right) = |+\rangle|\psi\rangle$$

If the input state is $|\phi\rangle$: Before controlled U, the state is

$$|+\rangle|\phi\rangle = \frac{1}{2}\left(|0\rangle|x\rangle - |0\rangle|y\rangle + |1\rangle|x\rangle - |1\rangle|y\rangle\right)$$

After controlled U, the state is

$$\frac{1}{2}\left(|0\rangle|x\rangle - |0\rangle|y\rangle + |1\rangle|y\rangle - |1\rangle|x\rangle\right) = |-\rangle|\phi\rangle$$

Swappability $\to$ Distinguishability

Proof: Suppose U satisfies

$$U|x\rangle = a|y\rangle + c|x\rangle + f|w\rangle$$
$$U|y\rangle = b|x\rangle + d|y\rangle + g|z\rangle$$

where $|a+b|/2 = \Delta$. The probabilities of accepting $|\psi\rangle$ and $|\phi\rangle$ are

$$\Pr_\psi(|+\rangle) = \frac{1}{2} + \frac{1}{4}\Re\left(e^{i\theta}(a+b+c+d)\right)$$
$$\Pr_\phi(|+\rangle) = \frac{1}{2} + \frac{1}{4}\Re\left(e^{i\theta}(-a-b+c+d)\right).$$

The bias is

$$\Pr_\psi(|+\rangle) - \Pr_\phi(|+\rangle) = \frac{\Re(e^{i\theta}(a+b))}{2} \le \frac{|a+b|}{2} = \Delta$$

The equality is achieved when we set $\theta = -\arg(a+b)$. $\square$

Tightness

Theorem

For any $0 \leq \Delta \leq 1$*, there exist a pair of orthogonal n-qubit states* $|x\rangle$ *and* $|y\rangle$ *and a swapper* U *of size* $O(1)$ *that swaps them with fidelity* Δ*, but to build a swapper with fidelity* $\Delta + \omega\left(0.5^{n/3}\sqrt{\log n}\right)$ *requires* $\omega\left(2^{n/3}\right)$ *gates.*

Corollary

For any $0 \leq \Delta \leq 1$*, there exist a pair of n-qubit states* $|\psi\rangle$ *and* $|\phi\rangle$ *and a distinguisher* A *of size* $O(1)$ *that distinguishes them with bias* Δ*, but to build a distinguisher with bias* $\Delta + \omega\left(0.5^{n/3}\sqrt{\log n}\right)$ *requires* $\omega\left(2^{n/3}\right)$ *gates.*

Summary

For any two orthogonal states $|x\rangle$ and $|y\rangle$ and

$$|\psi\rangle = \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|y\rangle\,, \quad |\phi\rangle = \frac{1}{\sqrt{2}}|x\rangle - \frac{1}{\sqrt{2}}|y\rangle$$

$$\begin{tikzcd}
\begin{array}{c}\text{distinguishing } |\psi\rangle \text{ and } |\phi\rangle \\ \text{with bias } \Delta + \omega\left(0.5^{n/3}\sqrt{\log n}\right)\end{array} \arrow[r, leftrightarrow, "O(1)"] & \begin{array}{c}\text{swapping } |x\rangle \text{ and } |y\rangle \\ \text{with error } 1 - \left(\Delta + \omega\left(0.5^{n/3}\sqrt{\log n}\right)\right)\end{array} \\
\begin{array}{c}\text{distinguishing } |\psi\rangle \text{ and } |\phi\rangle \\ \text{with bias } \Delta\end{array} \arrow[u, "\begin{array}{c}\text{potentially} \\ \omega\left(2^{n/3}\right)\end{array}"] \arrow[r, leftrightarrow, "O(1)"] & \begin{array}{c}\text{swapping } |x\rangle \text{ and } |y\rangle \\ \text{with error } 1 - \Delta\end{array} \arrow[u, "\begin{array}{c}\text{potentially} \\ \omega\left(2^{n/3}\right)\end{array}"']
\end{tikzcd}$$

Tightness: Background

Lemma

For random n-qubit states $|x\rangle$ and $|y\rangle$, $Pr\left(|\langle x \mid y\rangle| \geq \varepsilon\right) \leq e^{-\varepsilon^2(2^n-1)}$.

The probability is *doubly* exponentially small in *n*.

Lemma

For random n-qubit states $|x\rangle$ and $|y\rangle$, the probability that we can construct a circuit U such that $\langle y| U |x\rangle \geq \varepsilon$, for some ε of order $O(0.5^{n/3}\sqrt{\log n})$, using only $O(2^{n/3})$ gates from a universal gate set of size $n^{O(1)}$, is $0.5^{O(2^{n/3}\log n)}$.

The probability is still *doubly* exponentially small in *n*.

Tightness: Proof (1/3)

If we randomly sample 8 states $\{\psi_0, \psi_1, \cdots \psi_7\}$ from $\mathbb{C}^{2^{n-3}}$, they will be pairwise *almost* orthogonal with high probability. We could make them orthogonal by adding 3 index qubits, i.e.

$$\left|\bar{k}\right\rangle = |k\rangle \otimes |\psi_k\rangle \, , k \in \{0, 1\}^3 \, .$$

Based on $\left\{\left|\bar{k}\right\rangle\right\}$ we can construct a orthonormal basis of $\mathbb{C}^{2^n}$.

Tightness: Proof (2/3)

For the following two orthogonal states:

$$|x\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3}|\bar{k}\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle + |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{6}\rangle$$

$$|y\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3}i^k\,|\bar{k}\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle - |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{7}\rangle\,,$$

the following swapper of size $O(1)$ achieves fidelity $(a+b)/2$:

$$U = \left(\sum_{k=0}^{3} i^k\,|k\rangle\langle k| + |4\rangle\langle 4| - |5\rangle\langle 5| + |6\rangle\langle 6| + |7\rangle\langle 7|\right)\otimes \mathbb{I}_{2^{n-3}}$$

Tightness: Proof (3/3)

Consider any swapper U of size $O\left(2^{n/3}\right)$ and its representation in a basis where $\left\{\left|\bar{k}\right\rangle\right\}$ are the first 8 basis vectors. Let V be identical to U in the first 8×8 entries and 0 everywhere else. V achieves the same fidelity as U:

$$d' = \langle y| U |x\rangle = \langle y| V |x\rangle , \quad b' = \langle x| U |y\rangle = \langle x| V |y\rangle$$

For any $i \neq j$, with an overwhelming probability,

$$\left|\langle\bar{i}| V |\bar{j}\rangle\right| = O\left(0.5^{n/3} \log n\right) ,$$

which means that

$$V = \sum_{k=0}^{7} \beta_k e^{i\theta_k} \left|\bar{k}\right\rangle \left\langle\bar{k}\right| \pm O\left(0.5^{n/3} \log n\right) , \text{ where } 0 \leq \beta_k \leq 1.$$

Therefore,

$$\left|d' + b'\right| \leq |a + b| + O\left(0.5^{n/3} \log n\right)$$