University of Illinois Urbana-Champaign
CS 498QC Introduction to Quantum Computing

Author: Wenqi He (wenqihe2)
Date: Dec 4, 2023

PROJECT
1

CS 498QC Project Report

This report is a review of *On the Hardness of Detecting Macroscopic Superpositions* [1] by Scott Aaronson, Yosi Atia and Leonard Susskind.

1.1 Introduction

When we talk about "quantum", we are usually interested in systems where we can exploit the distinctly quantum phenomena of interference and entanglement, and not just everyday objects that, despite being governed by quantum mechanics, do not exhibit any "quantumness". A natural question then is: Where does the quantum world end and the classical world begin?

The emergence of classicality has been well explained by the theory of decoherence, which says that a system can be entangled with the environment in such a way that, when we "trace out" the environment, the reduced density matrix of the system describes a classical mixture governed by classical probabilities, even though the system and the environment as a whole remains in pure states following unitary evolutions.

This paper offers an additional explanation from a computer science perspective that doesn't involve any entanglement with the environment. The authors postulate that classicality could also arise from the practical infeasibility of distinguishing certain pure superpositions from classical mixtures. Such pure states could be considered, in the authors' words, "*effectively decohered*". This means that, not only are we unable to observe interference for such superpositions, we are also unable to prepare them.

1.2 Definitions

1.2.1 Equal Superposition and Equal Mixture

This paper focused on two equal superpositions and the equal mixture of orthogonal states $|x\rangle$ and $|y\rangle$:

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

Note that there is a symmetry:

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

1.2.2 Distinguishing

What does it mean to distinguish two states? Suppose we apply a distinguishing circuit to the input state and then measure the first qubit, and we accept the input if the outcome is $|0\rangle$. If the difference between the probabilities of accepting two different states is larger than any possible errors in estimating the probabilities, then the circuit can successfully distinguish those two states. Furthermore, we can focus on distinguishing between superpositions, because the ability to distinguish two different equal superpositions implies the ability to distinguish an equal superposition and an equal mixture: If the probability of accepting $|\psi\rangle$ is p_1 and the probability of accepting $|\phi\rangle$ is p_2, then the probability of accepting the equal mixture is

$$\begin{aligned}
&\langle 0|\,\mathrm{tr}_{env}\left(U\rho_{mixed}U^\dagger\right)|0\rangle \\
&= \langle 0|\,\mathrm{tr}_{env}\left(U\left(\frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{2}|\phi\rangle\langle\phi|\right)U^\dagger\right)|0\rangle \\
&= \frac{1}{2}\langle 0|\,\mathrm{tr}_{env}\left(U|\psi\rangle\langle\psi|U^\dagger\right)|0\rangle + \frac{1}{2}\langle 0|\,\mathrm{tr}_{env}\left(U|\phi\rangle\langle\phi|U^\dagger\right)|0\rangle \\
&= \frac{p_1+p_2}{2}
\end{aligned}$$

Definition 1.1. A distinguisher for $|\psi\rangle$ and $|\phi\rangle$ with bias Δ is a circuit U that accepts $|\psi\rangle$ with probability p and accepts $|\phi\rangle$ with probability $p-\Delta$, namely,

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

where

$$|a|^2 = p, \quad |b|^2 = 1-p, \quad |c|^2 = p-\Delta, \quad |d|^2 = 1-p+\Delta.$$

Such a distinguisher accepts the equal mixture of $|x\rangle$ and $|y\rangle$ with probability $p-\Delta/2$.

1.2.3 Swapping

The main result of the paper is the discovery that distinguishing a superposition from a classical mixture of two orthogonal states is as hard as swapping the two orthogonal states. But what exactly do we mean by "hardness"? Originally, Susskind conjectured that the hardness is measured by relative complexity.

Definition 1.2. The relative complexity $\mathcal{C}_\varepsilon(|x\rangle, |y\rangle)$ of two states $|x\rangle$ and $|y\rangle$ is the minimum number of gates needed for a circuit U that satisfies

$$|\langle y|U|x\rangle| \geq 1-\varepsilon$$

Aaronson showed that the conjecture is true only if we use a symmetrical "swap complexity" instead.

DEFINITION 1.3. A swapper for $|x\rangle$ and $|y\rangle$ with error $\varepsilon \in [0,1]$ is a circuit U that satisfies

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

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

DEFINITION 1.4. The swap complexity $\mathcal{S}_\varepsilon(|x\rangle, |y\rangle)$ of two states $|x\rangle$ and $|y\rangle$ is the minimum number of gates needed for a circuit U that satisfies

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

i.e., a swapper for $|x\rangle$ and $|y\rangle$ with error ε.

1.3 Equivalence Theorem

The equivalence theorem is the main result of this paper. The authors showed that the circuit complexity of distinguishing $|\psi\rangle$ and $|\phi\rangle$ with bias Δ, or equivalently, of distinguishing $|\psi\rangle$ or $|\phi\rangle$ from the equal mixture of $|x\rangle$ and $|y\rangle$ with bias $\Delta/2$, is the same as the circuit complexity of swapping $|x\rangle$ and $|y\rangle$ with error $\varepsilon = 1 - \Delta$.

The implication is that, when it is practically infeasible (e.g. due to thermodynamical reasons) to build an effective swapper for two orthogonal macroscopic states $|x\rangle$ and $|y\rangle$, it would also be infeasible to distinguish an equal superposition of $|x\rangle$ and $|y\rangle$ from the equal mixture of $|x\rangle$ and $|y\rangle$.

1.3.1 Distinguishability Implies Swappability

THEOREM 1.5. *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.*

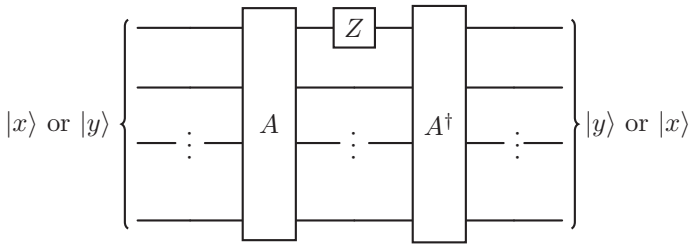
Proof. Suppose we have a distinguisher A for $|\psi\rangle$ and $|\phi\rangle$, such that

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

where

$$|a|^2 = p, \quad |b|^2 = 1 - p, \quad |c|^2 = p - \Delta, \quad |d|^2 = 1 - p + \Delta,$$

then the following circuit swaps $|x\rangle$ and $|y\rangle$ with fidelity Δ:



Let Z_0 represent a Z gate applied on the first qubit, then

$$\begin{aligned}
A|x\rangle &= \frac{1}{\sqrt{2}}(A|\psi\rangle + A|\phi\rangle) = \frac{1}{\sqrt{2}}\left[a|0\rangle|g_0(\psi)\rangle + b|1\rangle|g_1(\psi)\rangle + c|0\rangle|h_0(\phi)\rangle + d|1\rangle|h_1(\phi)\rangle\right] \\
Z_0A|x\rangle &= \frac{1}{\sqrt{2}}\left[-a|0\rangle|g_0(\psi)\rangle + b|1\rangle|g_1(\psi)\rangle - c|0\rangle|h_0(\phi)\rangle + d|1\rangle|h_1(\phi)\rangle\right] \\
A|y\rangle &= \frac{1}{\sqrt{2}}(A|\psi\rangle - A|\phi\rangle) = \frac{1}{\sqrt{2}}\left[a|0\rangle|g_0(\psi)\rangle + b|1\rangle|g_1(\psi)\rangle - c|0\rangle|h_0(\phi)\rangle - d|1\rangle|h_1(\phi)\rangle\right] \\
Z_0A|y\rangle &= \frac{1}{\sqrt{2}}\left[-a|0\rangle|g_0(\psi)\rangle + b|1\rangle|g_1(\psi)\rangle + c|0\rangle|h_0(\phi)\rangle - d|1\rangle|h_1(\phi)\rangle\right] \\
a &= \langle y|U|x\rangle = \langle y|A^\dagger Z_0 A|x\rangle \\
&= -\Delta + \frac{1}{2}\left[ac\left(\langle h_0(\phi)\,|\,g_0(\psi)\rangle - \langle g_0(\psi)\,|\,h_0(\phi)\rangle\right) + bd\left(\langle g_1(\psi)\,|\,h_1(\phi)\rangle - \langle h_1(\phi)\,|\,g_1(\psi)\rangle\right)\right] \\
b &= \langle x|U|y\rangle = \langle x|A^\dagger Z_0 A|y\rangle = a^* \\
&= -\Delta + \frac{1}{2}\left[ac\left(\langle g_0(\psi)\,|\,h_0(\phi)\rangle - \langle h_0(\phi)\,|\,g_0(\psi)\rangle\right) + bd\left(\langle g_1(\phi(\,|\,g_1(\psi)\rangle - \langle g_1(\psi)\,|\,h_1(\phi)\rangle\right)\right].
\end{aligned}$$

Finally, the fidelity of the swapper is

$$\frac{|a+b|}{2} = \frac{|-2\Delta|}{2} = \Delta.$$

□

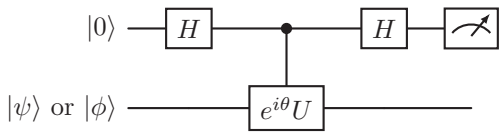
1.3.2 Swappability Implies Distinguishability

THEOREM 1.6. *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.*

Proof. Suppose we have a swapper U, such that

$$U|x\rangle = a|y\rangle + c|x\rangle + f|w\rangle, \quad U|y\rangle = b|x\rangle + d|y\rangle + g|z\rangle, \quad \frac{|a+b|}{2} = \Delta,$$

then the following circuit distinguishes $|\psi\rangle$ and $|\phi\rangle$ with bias Δ:



If the initial state is $|\psi\rangle$, the state after applying the controlled $e^{i\theta}U$ gate is

$$A|\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle|\psi\rangle + |1\rangle e^{i\theta}U|\psi\rangle\right] = \frac{1}{2}\left[|+\rangle|\psi\rangle + |-\rangle|\psi\rangle + |+\rangle e^{i\theta}U|\psi\rangle - |-\rangle e^{i\theta}U|\psi\rangle\right]$$

The reduced density matrix of the first qubit is

$$\begin{aligned}
\rho_\psi &= \mathrm{tr}_{env}\left(A\left|\psi\right\rangle\left\langle\psi\right|A^\dagger\right) \\
&= \frac{1}{4}\left[\left|+\right\rangle\left\langle+\right|\otimes\left(1+\mathrm{tr}\left(\left|\psi\right\rangle\left\langle\psi\right|e^{-i\theta}U^\dagger\right)+\mathrm{tr}\left(e^{i\theta}U\left|\psi\right\rangle\left\langle\psi\right|\right)+1\right)+\cdots\right] \\
&= \frac{1}{4}\left[\left|+\right\rangle\left\langle+\right|\otimes\left(1+\left\langle\psi\right|e^{-i\theta}U^\dagger\left|\psi\right\rangle+\left\langle\psi\right|e^{i\theta}U\left|\psi\right\rangle+1\right)+\cdots\right] \\
&= \left[\frac{1}{2}+\frac{1}{2}\Re\left(\left\langle\psi\right|e^{i\theta}U\left|\psi\right\rangle\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}\left(\left\langle x\right|+\left\langle y\right|\right)U\left(\left|x\right\rangle+\left|y\right\rangle\right)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}\left(\left\langle x\right|+\left\langle y\right|\right)\left(a\left|y\right\rangle+c\left|x\right\rangle+f\left|w\right\rangle+b\left|x\right\rangle+d\left|y\right\rangle+g\left|z\right\rangle\right)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}(a+b+c+d)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots .
\end{aligned}$$

The probability of accepting $\left|\psi\right\rangle$ is

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

Similarly, for input state $\left|\phi\right\rangle$,

$$\begin{aligned}
\rho_\phi &= \left[\frac{1}{2}+\frac{1}{2}\Re\left(\left\langle\psi\right|e^{i\theta}U\left|\psi\right\rangle\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}\left(\left\langle x\right|-\left\langle y\right|\right)U\left(\left|x\right\rangle-\left|y\right\rangle\right)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}\left(\left\langle x\right|-\left\langle y\right|\right)\left(a\left|y\right\rangle+c\left|x\right\rangle+f\left|w\right\rangle-b\left|x\right\rangle-d\left|y\right\rangle-g\left|z\right\rangle\right)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots \\
&= \left[\frac{1}{2}+\frac{1}{4}\Re\left(e^{i\theta}(-a-b+c+d)\right)\right]\left|+\right\rangle\left\langle+\right|+\cdots .
\end{aligned}$$

The probability of accepting $\left|\phi\right\rangle$ is

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

Finally, the bias of the distinguisher is

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

By setting $\theta=-\arg(a+b)$, we could achieve

$$\Pr_\psi(\left|+\right\rangle)-\Pr_\phi(\left|+\right\rangle)=\frac{|a+b|}{2}=\Delta.$$

□

1.3.3 Perfect Swappability and Distinguishability

To understand the circuits in the proof of the equivalence theorem, it's helpful to observe how swapping and distinguishing operate in the perfect case, when $\Delta = 1$ and $\varepsilon = 0$.

1.3.3.1 Perfect Swapper from Perfect Distinguisher

Suppose we have a perfect distinguisher A, i.e.

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

With swapper $U = A^\dagger Z_0 A$,

$$\begin{aligned}
A|x\rangle &= A\left(\frac{|\psi\rangle + |\phi\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle|g_0(\psi)\rangle + |1\rangle|h_1(\phi)\rangle\right) \\
A|y\rangle &= A\left(\frac{|\psi\rangle - |\phi\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}\left(|0\rangle|g_0(\psi)\rangle - |1\rangle|h_1(\phi)\rangle\right) \\
Z_0 A|x\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|g_0(\psi)\rangle - |1\rangle|h_1(\phi)\rangle\right) = A|y\rangle \\
Z_0 A|y\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle|g_0(\psi)\rangle + |1\rangle|h_1(\phi)\rangle\right) = A|x\rangle \\
U|x\rangle &= A^\dagger Z_0 A|x\rangle = |y\rangle \\
U|y\rangle &= A^\dagger Z_0 A|y\rangle = |x\rangle.
\end{aligned}$$

U is indeed a perfect swapper.

1.3.3.2 Perfect Distinguisher from Perfect Swapper

Suppose we have a perfect swapper U such that $U|x\rangle = |y\rangle$ and $U|y\rangle = |x\rangle$.

- If the input state is $|\psi\rangle$, the joint state with the ancilla qubit 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 applying the controlled-U (with $\theta = 0$), 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 the 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 the controlled-U, the state is

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

The circuit is indeed a perfect distinguisher.

1.4 Tightness Theorem

The equivalence theorem only gives us a lower bound — that is, we could convert a swapper with fidelity Δ into a distinguisher with bias *at least* Δ, and vice versa. But is it possible to do better with the same asymptotic circuit complexity? In this paper, the authors showed that the answer is not always. (This seems to be a relatively weak statement).

1.4.1 Vastness of Hilbert Space

With a non-trivial number of qubits, if we uniformly sample two random states, they will almost always be almost orthogonal. More formally,

LEMMA 1.7. *For any random n-qubit states $|x\rangle$ and $|y\rangle$, $\forall \varepsilon > 0$. $Pr\left(|\langle x \,|\, y\rangle| \geq \varepsilon\right) \leq e^{-\varepsilon^2(2^n-1)}$. (Note that this probability is doubly-exponentially small in the number of qubits.)*

The following proof is given in [2].

Proof. Let $N = 2^n$. Suppose we sample two vectors from $\mathbb{C}^N$ with a Gaussian probability measure

$$\Pr(z) = \frac{1}{\pi^N} e^{-\|z\|^2},$$

and then normalize them into $|x\rangle$ and $|y\rangle$. WLOG, let $|y\rangle = \dfrac{z}{\|z\|}$ and $|x\rangle = |0^n\rangle$.

$$\begin{aligned}
&Pr\left(|\langle y \,|\, x\rangle| \geq \varepsilon\right) = Pr\left(|z_0| \geq \varepsilon \|z\|\right) \\
&= \int_{|z_0| \geq \varepsilon\|z\|} \frac{1}{\pi^N} e^{-\|z\|^2} dx_0 dy_0 \cdots dx_{N-1} dy_{N-1} \\
&= \int_{|r_0| \geq \varepsilon\|z\|} \frac{1}{\pi^N} e^{-\|z\|^2} r_0 dr_0 d\theta_0 \cdots r_{N-1} dr_{N-1} d\theta_{N-1} \\
&= \left(\prod_{i=0}^{N-1} \frac{1}{2\pi} \int_0^{2\pi} d\theta_i\right) \int_{r_0,\cdots,r_{N-1},|r_0|\geq\varepsilon\|z\|} 2^N e^{-\left(r_0^2+\cdots+r_{N-1}^2\right)} r_0 dr_0 \cdots r_{N-1} dr_{N-1} \\
&= \int_{r_1,\cdots,r_{N-1}=0}^{\infty} 2^{N-1} e^{-\left(r_1^2+\cdots+r_{N-1}^2\right)} \left(\int_{r_0=\sqrt{\frac{\varepsilon^2\left(r_1^2+\cdots+r_{N-1}^2\right)}{1-\varepsilon^2}}}^{\infty} 2e^{-r_0^2} r_0 dr_0 \right) r_1 dr_1 \cdots r_{N-1} dr_{N-1} \\
&= \int_{r_1,\cdots,r_{N-1}=0}^{\infty} 2^{N-1} e^{-\left(r_1^2+\cdots+r_{N-1}^2\right)} e^{-\varepsilon^2\left(r_1^2+\cdots+r_{N-1}^2\right)/\left(1-\varepsilon^2\right)} r_1 dr_1 \cdots r_{N-1} dr_{N-1} \\
&= \int_{r_1,\cdots,r_{N-1}=0}^{\infty} 2^{N-1} e^{-\left(r_1^2+\cdots+r_{N-1}^2\right)/\left(1-\varepsilon^2\right)} r_1 dr_1 \cdots r_{N-1} dr_{N-1} = \prod_{i=1}^{N-1} \int_{r_i=0}^{\infty} 2e^{-r_i^2/\left(1-\varepsilon^2\right)} r_i dr_i \\
&= \left(1-\varepsilon^2\right)^{N-1} \leq e^{-\varepsilon^2(N-1)} = e^{-\varepsilon^2(2^n-1)}
\end{aligned}$$

□

1.4.2 Exponential Relative Complexity of Random States

This paper proved an even stronger statement: Given two random states, even if we are allowed to rotate one of them with an exponential-sized circuit, they will still be almost

orthogonal with an overwhelming probability. (The probability of them not being almost orthogonal is still *doubly*-exponentially small.)

THEOREM 1.8. *With probability* $1 - 0.5^{O(2^{n/3}\log n)}$ *, a random* n*-qubit state* $|x\rangle$ *cannot be transformed by a circuit* U *with only* $O(2^{n/3})$ *gates such that* $\langle y|\, U\, |x\rangle \geq \varepsilon$*, for some* $\varepsilon = O(0.5^{n/3}\sqrt{\log n})$*.*

Proof. With a universal gate set of size g and M gates, we could make g^M different gates. By Boole's inequality, the probability that at least one of the gates U_i achieves $|\langle y|\, U_i\, |x\rangle| \geq \varepsilon$ is at most

$$g^M \cdot e^{-\varepsilon^2(2^n-1)} = 2^{M\log g - \varepsilon^2(2^n-1)\log e}.$$

We could set ε to be as large as $\sqrt{M\log g/2^n}$ and still keep the order of the probability unchanged:

$$2^{M\log g\cdot[1-\log e(1-1/2^n)]}.$$

When $g = n^{O(1)}$, $M = O(2^{n/3})$, $\varepsilon = O(0.5^{n/3}\log n)$, the probability is $0.5^{O(2^{n/3}\log n)}$. □

1.4.3 Exponential Gap of Swap Complexity

The authors demonstrated the tightness of the equivalence theorem with an explicit example that, with an overwhelming probability, requires at least an exponential number of gates just to make an exponentially small improvement.

THEOREM 1.9. *For any* $0 \leq a \leq b \leq 1$*, there exist a pair of orthogonal* n*-qubit states* $|x\rangle$ *and* $|y\rangle$ *and a swapper* U *of size* $O(1)$ *such that* $\langle y|\, U\, |x\rangle = a$ *and* $\langle x|\, U\, |y\rangle = b$*, but to build a swapper* U' *such that* $\langle y|\, U'\, |x\rangle = a'$ *and* $\langle x|\, U'\, |y\rangle = b'$ *and* $|a'+b'| \geq |a+b| + \omega\left(0.5^{n/3}\sqrt{\log n}\right)$ *requires* $\omega\left(2^{n/3}\right)$ *gates. Equivalently, 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* $O(1)$ *such that* A *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.*

Proof. We can randomly sample 8 states $\{\psi_0, \psi_1, \cdots \psi_7\}$ from $\mathbb{C}^{2^{n-3}}$. We have shown that it's practically impossible to implement a unitary U with only $O\left(2^{n/3}\right)$ gates such that for some $i \neq j$,

$$|\langle\psi_i|\, U\, |\psi_j\rangle| \geq \varepsilon, \text{ for some } \varepsilon = \omega\left(0.5^{n/3}\sqrt{\log n}\right).$$

We can add 3 index qubits to make these states *actually* pairwise orthogonal:

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

Before analyzing the general case, we first show that fidelity $(a+b)/2$ is indeed achievable with $O(1)$ gates. Consider the unitary

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

and the two orthogonal states

$$|x\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3}\left|\bar{k}\right\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle + |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{6}\rangle$$
$$|y\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3} i^k\left|\bar{k}\right\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle - |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{7}\rangle\,.$$

We can verify that

$$U|x\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3} i^k\left|\bar{k}\right\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle - |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{6}\rangle$$
$$U|y\rangle = \sqrt{a-b}\left(\frac{1}{2}\sum_{k=0}^{3}(-1)^k\left|\bar{k}\right\rangle\right) + \sqrt{b}\left(\frac{|\bar{4}\rangle + |\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\,|\bar{7}\rangle$$
$$\langle y|\,U\,|x\rangle = (a-b) + b + 0 = a$$
$$\langle x|\,U\,|y\rangle = 0 + b + 0 = b.$$

Since U only acts on the first 3 qubits, it requires only $O(1)$ gates.

Now consider an arbitrary U' with $O(2^{n/3})$ gates. We could choose an orthonormal basis of $\mathbb{C}^{2^n}$ where $\left\{\left|\bar{k}\right\rangle\right\}$ are the first 8 basis vectors. Since both $|x\rangle$ and $|y\rangle$ are superpositions of $\left\{\left|\bar{k}\right\rangle\right\}$, only the first 8×8 entries of the matrix contribute to the final result, so instead of U', we could just consider the matrix V that is identical to U' in the first 8×8 entries and 0 everywhere else. As shown before, with an overwhelming probability, we are only able to achieve

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

which means that V is approximately diagonal, and can be expressed as

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

We can now calculate the fidelity of U':

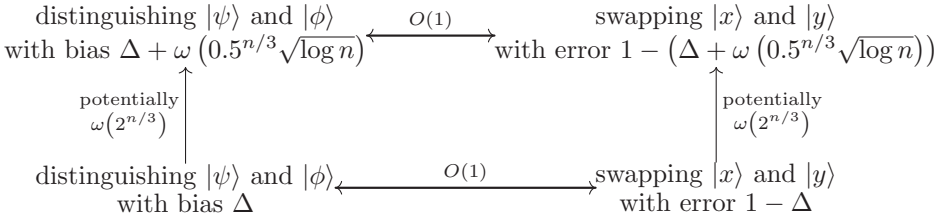
$$V|x\rangle = \sqrt{a-b}\left(\frac{\beta_0 e^{i\theta_0}|\bar{0}\rangle + \beta_1 e^{i\theta_1}|\bar{1}\rangle + \beta_2 e^{i\theta_2}|\bar{2}\rangle + \beta_3 e^{i\theta_3}|\bar{3}\rangle}{2}\right)$$
$$+ \sqrt{b}\left(\frac{\beta_4 e^{i\theta_4}|\bar{4}\rangle + \beta_5 e^{i\theta_5}|\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\beta_6 e^{i\theta_6}|\bar{6}\rangle \pm O\left(0.5^{n/3}\log n\right)$$
$$V|y\rangle = \sqrt{a-b}\left(\frac{\beta_0 e^{i\theta_0}|\bar{0}\rangle + i\beta_1 e^{i\theta_1}|\bar{1}\rangle - \beta_2 e^{i\theta_2}|\bar{2}\rangle - i\beta_3 e^{i\theta_3}|\bar{3}\rangle}{2}\right)$$
$$+ \sqrt{b}\left(\frac{\beta_4 e^{i\theta_4}|\bar{4}\rangle - \beta_5 e^{i\theta_5}|\bar{5}\rangle}{\sqrt{2}}\right) + \sqrt{c}\beta_7 e^{i\theta_7}|\bar{7}\rangle \pm O\left(0.5^{n/3}\log n\right)$$

$$
\begin{aligned}
a' &= \langle y| U' |x\rangle = \langle y| V |x\rangle \\
&= (a-b)\left(\frac{\beta_0 e^{i\theta_0} - i\beta_1 e^{i\theta_1} - \beta_2 e^{i\theta_2} + i\beta_3 e^{i\theta_3}}{4}\right) + b\left(\frac{\beta_4 e^{i\theta_4} - \beta_5 e^{i\theta_5}}{2}\right) \pm O\left(0.5^{n/3}\log n\right) \\
b' &= \langle x| U' |y\rangle = \langle x| V |y\rangle \\
&= (a-b)\left(\frac{\beta_0 e^{i\theta_0} + i\beta_1 e^{i\theta_1} - \beta_2 e^{i\theta_2} - i\beta_3 e^{i\theta_3}}{4}\right) + b\left(\frac{\beta_4 e^{i\theta_4} - \beta_5 e^{i\theta_5}}{2}\right) \pm O\left(0.5^{n/3}\log n\right) \\
|a'+b'| &= \left|(a-b)\left(\frac{\beta_0 e^{i\theta_0} - \beta_2 e^{i\theta_2}}{2}\right) + b\left(\beta_4 e^{i\theta_4} - \beta_5 e^{i\theta_5}\right)\right| \pm O\left(0.5^{n/3}\log n\right) \\
&\leq (a-b)\left|\frac{\beta_0 e^{i\theta_0} - \beta_2 e^{i\theta_2}}{2}\right| + b\left|\beta_4 e^{i\theta_4} - \beta_5 e^{i\theta_5}\right| + O\left(0.5^{n/3}\log n\right) \\
&\leq (a-b) + 2b + O\left(0.5^{n/3}\log n\right) \\
&= |a+b| + O\left(0.5^{n/3}\log n\right)
\end{aligned}
$$

□

1.5 Conclusion

Using straightforward constructive proofs, the authors showed two main results: The equivalence theorem, discussed in Section 1.3 of this report, establishes the relation between the asymptotic circuit complexities of distinguishing and swapping. The tightness theorem, discussed in Section 1.4 of this report, describes how the circuit complexities could be extremely sensitive to the error parameter ε (or equivalently, Δ). These results can be summarized as the following diagram:



Again, as we have shown in Section 1.2, the distinguishability between $|\psi\rangle$ and $|\phi\rangle$ implies the distinguishability between either of these two pure superpositions and the equal classical mixture of $|x\rangle$ and $|y\rangle$ (or equivalently, of $|\psi\rangle$ and $|\phi\rangle$).

References

[1] S. Aaronson, Y. Atia, and L. Susskind. On the hardness of detecting macroscopic superpositions, 2020.

[2] S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. In *Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity*, CCC '07, page 115–128, USA, 2007. IEEE Computer Society.