No-Existence Of Generalize Diffusion.

David Ponarovsky

July 25, 2022

Preamble One of the most promised applications of quantum computation is the Amplitude Amplification algorithm [Bra+02], In which, one can transform a known state $|\Psi\rangle$ with probability a to measure a $|i\rangle$ to a state in which the desired measurement obtained with probability grater than $\frac{1}{2}$ at the cost of less than $\sqrt{a}$ sort of Grover iterations. A critical requirement for that precedure is to have the ability to generate a copeis of the initial state, formulated in [Bra+02] as holding algorithm $\mathcal{A}$, which does not make any mausrements, such $\mathcal{A}|0\rangle = |\Psi\rangle$. One question that might rise is whether the above can be done given a single entity of the state. We show that there is no operator that given two state $|\psi\rangle, |\phi\rangle$ compute the transformation:

$$D|\psi\rangle|\phi\rangle = |\psi\rangle(\mathbb{I} - 2|\psi\rangle\langle\psi|)|\phi\rangle$$

We name the gate above the *Generalize Diffusion* gate, As if such gate were exists it could be used instand of the projection operator to simulate the amplitude amplification procedure. The contradiction of the existence follows by showing that using D two players can compute the disjoints of their sets in single round and $O(\sqrt{n})$ communication complexity, which shown by Braverman to be impossible [Bra+18].

Quantum Communication Complexity of Disjointness. Consider the following communication problem. As inputs Alice gets an x and Bob get a y, where $x, y \in \{0,1\}^n$, and by exchanging information they want to determine if there is an index k with $x_k = y_k = 1$ or not. In other words, if x encodes the set $A = \{k | x_k = 1\}$, and y encodes $B = \{k | y_k = 1\}$, then Alice and Bob want to determine whether $A \cap B$ is empty or not.

The classical randomized communication complexity of this problem is $\mathcal{O}(n)$. Assuming Alice and Bob can exchange quantum messages, It is known that Alice and bob can solve the task correctly with probability greater than $2/3$ by exchanging at most $\mathcal{O}(\sqrt{n}\log n)$ qubits **[COMMENT]** add ciation of the original solution.

The reduction. Assume by way of contradiction the existance of D defined above. Let $x^{(j)}$ be the j-th $\sqrt{n}$-block of x, e.g $x^{(j)} = x_{j\sqrt{n}}, x_{j\sqrt{n}+1} \dots, x_{(j+1)(\sqrt{n})-1}$. And denote by $|\psi_x\rangle \in \mathcal{H}_2^{\bigotimes \sqrt{n}} \bigotimes \mathcal{H}_{\sqrt{n}}$ the uniform superposition state over the $x^{(j)}$-'s "tensored" with $\sqrt{n}$-qudit (which will correspond to the block number).

$$|\psi_x\rangle = \frac{1}{n^{\frac{1}{4}}} \sum_{j}^{\sqrt{n}} |x^{(j)}\rangle |j\rangle$$

Note that the encoding of $|\psi_x\rangle$ require only $\sqrt{n} + \log(\sqrt{n})$ qubits. Clearly both Alice and Bob can generate the states $|\psi_x\rangle, |\psi_y\rangle$, then Bob sends he's share to Alice. We know that there is a classical circuit with logarithmic depth in $\sqrt{n}$ that act over the pure states $|x^{(j)}\rangle|j\rangle, |y^{(k)}\rangle|k\rangle$ and decides whether

$$(j = k) \bigwedge \left(\bigvee_{i \in [\sqrt{n}]} x_i^{(j)} \wedge y_i^{(k)} \right)$$

Denote it by C and by U the phase flip controlled by C i.e. $U|i\rangle = (-1)^{C(i)}|i\rangle$.

Claim. *Recall the operator $\mathbf{Q} = -\mathcal{A}\mathbf{S}_0\mathcal{A}^{-1}\mathbf{S}_\chi$ defined in [Bra+02], such that $\mathcal{A}|0\rangle = |\Psi\rangle = |\psi_x\rangle|\psi_y\rangle$ and consider the generalize diffusion gate D, Then it holds that for any state $|\phi\rangle \in \mathcal{H}_\Psi$:*

$$(\mathbb{I} \otimes \mathbf{Q})|\psi_x\rangle|\psi_y\rangle|\phi\rangle = -D(\mathbb{I} \otimes U)|\psi_x\rangle|\psi_y\rangle|\phi\rangle$$

Proof. Let $|\Psi_0\rangle, |\Psi_1\rangle$ be the base which span $\mathcal{H}_\Psi$ and in addition $U|\Psi_0\rangle = |\Psi_0\rangle, U|\Psi_1\rangle = -|\Psi_1\rangle$.

First consider the case in which the diminsion of $\mathcal{H}_\Psi$ is exactly 1, If $|\Psi\rangle$ supported only on non-satisfaing states (i.e $|\Psi\rangle = |\Psi_0\rangle$) then it's clear that $I \otimes U$ act over the $|\Psi\rangle|\Psi\rangle$ as identity and therefore $-D(I \otimes U)$ act also as identity:

$$-D(I \otimes U)|\Psi\rangle|\Psi\rangle = -|\Psi\rangle(I - 2|\Psi\rangle\langle\Psi|)|\Psi\rangle = |\Psi\rangle|\Psi\rangle$$

Similar calculation yields that the action is tricial also when $\mathcal{H}_\Psi$ supported only over $|\Psi_1\rangle$.

It is left to show the equivaliance when $|\Psi\rangle$ supported both over $|\Psi_0\rangle$ and $|\Psi_1\rangle$. Then it follows that:

$$
\begin{aligned}
&-D\left(\mathbb{I}\otimes U\right)|\psi_x\rangle|\psi_y\rangle|\Psi_1\rangle = D|\psi_x\rangle|\psi_y\rangle|\Psi_1\rangle\\
&\quad |\psi_x\rangle|\psi_y\rangle\left(\mathbb{I}-2|\psi_x\rangle|\psi_y\rangle\langle\psi_x|\langle\psi_y|\right)|\Psi_1\rangle\\
&\quad |\psi_x\rangle|\psi_y\rangle\left(\mathbb{I}-2|\Psi\rangle\langle\Psi|\right)|\Psi_1\rangle\\
&\quad |\psi_x\rangle|\psi_y\rangle\left((1-2a)|\Psi_1\rangle-2a|\Psi_0\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
&-D\left(\mathbb{I}\otimes U\right)|\psi_x\rangle|\psi_y\rangle|\Psi_0\rangle = -D|\psi_x\rangle|\psi_y\rangle|\Psi_0\rangle\\
&\quad -|\psi_x\rangle|\psi_y\rangle\left(\mathbb{I}-2|\psi_x\rangle|\psi_y\rangle\langle\psi_x|\langle\psi_y|\right)|\Psi_0\rangle\\
&\quad -|\psi_x\rangle|\psi_y\rangle\left(\mathbb{I}-2|\Psi\rangle\langle\Psi|\right)|\Psi_0\rangle\\
&\quad -|\psi_x\rangle|\psi_y\rangle\left((-(2-2a))|\Psi_1\rangle+1-(2-2a)|\Psi_0\rangle\right)\\
&\quad |\psi_x\rangle|\psi_y\rangle\left((2-2a)|\Psi_1\rangle+(1-2a)|\Psi_0\rangle\right)\\
&\quad \square
\end{aligned}
$$

Now, it's clear that Alice, could simulate the **algqsearch** algorithm [Bra+02],

Theorem 3. *Quadratic speedup without knowing* **a** *There exists a quantum algorithm* ***algqsearch*** *with the following property. Let $\mathcal{A}$ be any quantum algorithm that uses no measurements, and let $\chi : \mathbb{N} \to \{0,1\}$ be any Boolean function. Let a denote the initial success probability of $\mathcal{A}$. Algorithm* ***algqsearch*** *finds a good solution using an expected number of applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$ which are in $\Theta(\sqrt{a})$ if $a > 0$, and otherwise runs forever.*

Proof of Theorem 1 Suppose that $A \cap B \neq \emptyset$ then, the support of $|\psi_x\rangle \otimes |\psi_y\rangle$ contain a state $|\phi\rangle$ which satisfies C, or in other words $a = |\langle\Psi_1|\Psi\rangle|^2 > 0$ and therefore by *Theorem 3* there is an explicit procedure which take a $\Theta(\sqrt{a})$ time in expectation, Hence for any $\varepsilon > 0$ we could construct a finite algorithm that fail with probability less than ε by rejecting runs that last longer than $\frac{1}{\varepsilon}$.

On the other hand, Consider the case when $A \cap B = \emptyset$ then $\Rightarrow a = 0 \Rightarrow \mathcal{H}_\Psi$ is 1-dimension space spanned only by $|\Psi_0\rangle$, and the operator $I - 2|\Psi\rangle\langle\Psi|$ act over the $|\Psi_0\rangle$ as identity and therefore after executing any number of iterations the probability to measure from $|\Psi_0\rangle$ will remain 1.

Summarize the above yields the following protocol,

1. Bob create $|\psi_x\rangle$ and send it to Alice.
2. Alice simulate **algqsearch** either the algorithm accept or either n^4 turns were passed.
3. If the algorithm accept then Alice return True otherwise Alice return False.

The protocol compute the disjointness in single round while requiring transmission of less than $\Theta(\sqrt{n})$ qubits. That in contrast to the known lower bound proved by Braverman [Bra+18]:

Theorem A *The r-round quantum communication complexity of Disjointness$_n$ is $\Omega\left(\frac{n}{r\log^8 r}\right)$.*

Open question.

References

[Bra+02] Gilles Brassard et al. *Quantum amplitude amplification and estimation.* 2002. DOI: 10.1090/conm/305/05215. URL: https://doi.org/10.1090%2Fconm%2F305%2F05215.

[Bra+18] Mark Braverman et al. "Near-Optimal Bounds on the Bounded-Round Quantum Communication Complexity of Disjointness". In: *SIAM Journal on Computing* 47.6 (2018), pp. 2277–2314. DOI: 10.1137/16M1061400. eprint: https://doi.org/10.1137/16M1061400. URL: https://doi.org/10.1137/16M1061400.