# Average-Case Quantum Advantage with Shallow Circuits

February 2020

# Refs

We present a result by François Le Gall [Le Gall, 2019], an average-case strengthening of the breakthrough result by Bravyi, Gosset, Koenig [Bravyi et al., Science, 2017].

# Shallow-depth circuits that we are concerned about

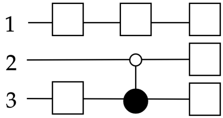
Fan-in = # inputs to a gate

**Definition: $NC^0$ circuits**

$NC^0$ circuits are constant-depth, bounded (gate) fan-in classical circuits

**Definition: $QNC^0$ circuits**

$QNC^0$ circuits are constant-depth, bounded (gate) fan-in quantum circuits



# Quantum advantage with shallow circuits (Bravyi et el.)

Bravyi et al. introduced the "2D HLF problem":

- No $NC^0$ circuit can solve the 2D HLF problem on $\geq \frac{7}{8}$ of inputs
- A $QNC^0$ circuit can solve the 2D HLF problem on all inputs
- First such **unconditional**, **non-oracular** separation in circuit model
  - Conditional: "If this conjecture is true, then our statement is true"
  - Oracular: "If we give the circuits access to some oracle computing a function, then we can separate them"

# Averge-case quantum advantage with shallow circuits

Le Gall shows the following for the "Graph State Measurement" problem:

- No randomized $NC^0$ circuit can solve GSM with average probability $\geq \frac{1}{\exp(\gamma\sqrt{n})}$ for some $\gamma > 0$
- A $QNC^0$ circuit can solve GSM on all inputs with certainty
- Separation for **exponentially small** classical correctness and **simpler** $QNC^0$ algorithm

# Relation problem

**Relation problem**

Input: $x \in \{0,1\}^m$. Output: Any $z \in R(x) \subseteq \{0,1\}^n$

# Preliminaries: Graph states

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

"Apply $Z$ to the target qubit if the control qubit is set"

## Definition: Graph state

For any graph $G = (V, E)$, let each $v \in V$ be a qubit initialized to $|0\rangle$. Apply $H$ to each $v \in V$, then for each $(u, v) \in E$ apply $CZ$ on $|\psi_u\rangle \otimes |\psi_v\rangle$. The resulting $|G\rangle$ is a graph state

Graph state measurement outcomes are **highly correlated**

# The extended graph

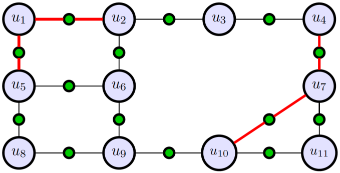
## Definition: Extended graph

For a graph $G$, the extended graph, $\overline{G}$, is obtained by introducing a new vertex on every edge. Let the new vertices be $V^*$

## Definition: $f$-covering

For $f : V \to \{0, 1\}$, an $f$-covering of $\overline{G}$ is a set of $\frac{|f|}{2}$ paths such that each $v \in V$ where $f(v) = 1$ appears only once as an endpoint

E.g., $f(u_2) = f(u_4) = f(u_5) = f(u_{10}) = 1$



# A general measurement process

Consider the following process:

**Process $P(G, f)$**

1. Construct the graph state corresponding to $\overline{G}$
2. For each $v \in V$: If $f(v) = 1$, then measure $v$ in $Y$-basis. For all other vertices in $V \cup V^*$, measure in $X$-basis.

Let $z_v \in \{0, 1\}$ be the measurement outcome of vertex $v$. $z_v = 0$ corresponds to $+1$ eigenvalue. $z_v = 1$ corresponds to $-1$ eigenvalue.

# Theorems of measurement parity for $P(G, f)$

**Theorem 3**

For any cycle $C$ of $\overline{G}$, with probability 1, $\bigoplus_{v \in C \cap V^*} z_v = 0$

**Theorem 4**

Let $|f|$ be even and $z_V = \bigoplus_{v \in V} z_v$. Then with probability 1,

$$z_V \oplus \bigoplus_{i=1}^{|f|/2} \bigoplus_{v \in p_i \cap V^*} z_v = \begin{cases} 0, & \text{if } |f| \mod 4 = 0 \\ 1, & \text{if } |f| \mod 4 = 2 \end{cases}$$

We will use these general graph state measurement theorems later.

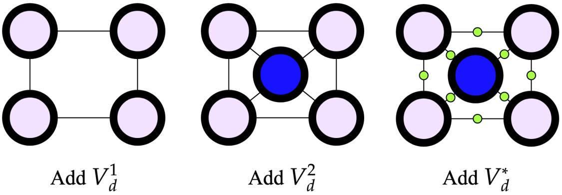
# The graph state that we use (small example)

## The Graph

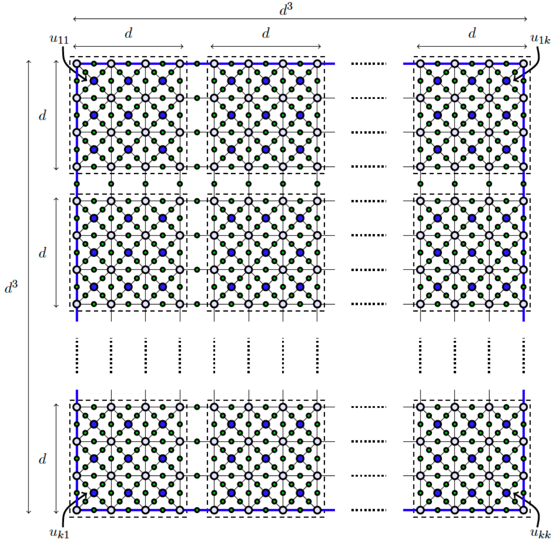
- $V_d^1$ is the vertices of a $d^3 \times d^3$ grid. Each $d \times d$ region is a "box"
- $V_d^2$ is the vertices we place inside every $1 \times 1$ square within every box
- $V_d = V_d^1 \cup V_d^2$.
- $V_d^*$ is the vertices of the extended graph

For convenience, denote $k := \sqrt{|V_d^2|}$ and $n := |V_d^1| + |V_d^2| + |V_d^*| = \Theta(d^6)$

Example of a $1 \times 1$ square in the grid:



# The graph state that we use (big example)




Blue outline is the **border**

# The computational problem that we solve (GSM)

Given $A = \{0,1\}^{k \times k}$ as input, define the following process

**Process $P_d(A)$**

1. Construct the graph state from $\overline{G_d}$ as before
2. For each $u_{ij} \in V_d^2$: If $A_{ij} = 1$, measure qubit $u_{ij}$ in the $Y$-basis. Otherwise, measure it in the $X$-basis.
3. For each $u \in V_d^1 \cup V_d^*$, measure $u$ in the $X$-basis.

Let $\Lambda_d(A) \subseteq \{0,1\}^n$ be the set of all possible measurement outcomes for $A$. The computational problem is to, given $A$ of size $m := k^2$, output any element of $\Lambda_d(A)$.

# GSM can be solved on $QNC^0$ circuit

## (Recall) Definition: Graph state

For any graph $G = (V, E)$, let each $v \in V$ be a qubit initialized to $|0\rangle$. Apply $H$ to each $v \in V$, then for each $(u, v) \in E$ apply $CZ$ on $|\psi_u\rangle \otimes |\psi_v\rangle$. The resulting $|G\rangle$ is a graph state

Idea: Follow the protocol for graph state construction, by definition:

- One layer of $H$ gates
- $O(1)$ layers of $CZ$ because of constant-degree vertices
- $O(1)$ layers for measurement

Correctness is clear

# The plan for showing a $NC^0$ circuit can't solve GSM

Show that any classical circuit solving GSM must satisfy unsatisfiable equations in its output

### Lemma 1

Consider the affine functions

$$q : \{0,1\}^3 \to \{0,1\} \text{ and } q_i : \{0,1\}^2 \to \{0,1\} \text{ for } i \in \{1,2,3\}$$

If $q_1(b_2, b_3) \oplus q_2(b_1, b_3) \oplus q_3(b_1, b_2) = 0$, then one of the following equations does not hold:

$$q(0,0,0) = 0 \tag{1}$$

$$q(0,1,1) \oplus q_1(1,1) = 1 \tag{2}$$

$$q(1,0,1) \oplus q_2(1,1) = 1 \tag{3}$$

$$q(1,1,0) \oplus q_3(1,1) = 1 \tag{4}$$

Next: find a cycle in our graph that exhibits these equations in $NC^0$

# Properties of classical circuit for GSM lower bounds

$C_d$ is a randomized classical circuit

- $m = k^2 = \Theta(d^6)$ input wires and $n = \Theta(d^6)$ output wires
- Fan-in $\leq 2$ and depth $\leq \frac{1}{8} \log_2 m$
- Assume that $n$ large enough so that $3n^{1/7} \leq d - 2$

Define the following wires:

- $x_{ij}$ wire receives the input bit $A_{ij}$
- $z_u$ wire outputs the measurement outcome for $u \in \overline{V_d}$

# Lightcones help quantify related input-output relationships

To model cause-and-effect relationships between input-output wires:

- For output wire $z_u$, define
  $L(z_u) = \{v \in V_d^2 :\ \text{value of } z_u \text{ depends on } x_v\}$
- Similarly, for input wire $x_v$, define
  $L(x_v) = \{u \in \overline{V_d} :\ \text{value of } z_u \text{ depends on } x_v\}$

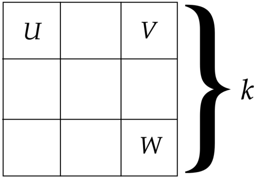
Let $\Gamma = \{u \in V_d^2 : L(x_u) > n^{1/7}\}$ (input wires with "big" lightcones)

- Via a simple counting argument, $|\Gamma| \leq O(n^{55/56})$

# Three distinct regions to form a cycle

Split grid into 9 regions. Then label input wires into groups $U$, $V$, $W$:

- $U$: top-left $\setminus\Gamma$
- $V$: top-right $\setminus\Gamma$
- $W$: bottom-right $\setminus\Gamma$




We'll connect $U$, $V$, $W$ in a cycle later on

# The lightcones from $U, V, W$ can be disjoint

Recall $d \times d$ boxes.

**Lemma 2**

The number of triples $(u, v, w) \in U \times V \times W$ where lightcones of $x_u, x_v, x_w$ intersect one another's boxes is $O(n^{2+10/21})$

**Lemma 3**

The number of triples $(u, v, w) \in U \times V \times W$ where the lightcones of $x_u, x_v, x_w$ are not pairwise disjoint is $O(n^{2+2/7})$

- Basic idea: Lightcones $L(x_u), L(x_v), L(x_w)$ have small size, $\leq n^{1/7}$
- $|U|, |V|, |W| = O(n) \implies |U \times V \times W| = O(n^3)$

# How to connect $(u, v, w)$ into a cycle correctly

Let $Box(x)$ be the $d \times d$ box that encloses vertex $x$

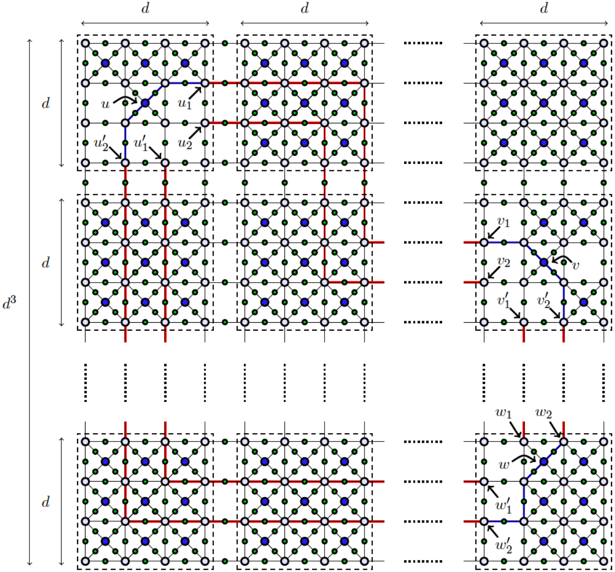
## Proposition 1

There is a $(u, v, w) \in U \times V \times W$ such that the following hold:

1. The lightcones of $x_u, x_v, x_w$ are pairwise disjoint
2. The lightcones of $x_u, x_v, x_w$ do not intersect one another's boxes
3. There is a cycle $C$ containing $u, v, w$ such that
    1. $C$ does not use any edge from the external border of $\overline{G_d}$, $\partial(\overline{G_d})$
    2. $C \cap V_d^2 = \{u, v, w\}$
    3. $q_{v \to w} \cap L(x_u) = \emptyset$, $q_{w \to u} \cap L(x_v) = \emptyset$, $q_{u \to v} \cap L(x_w) = \emptyset$, where $q_{a \to b}$ is the subpath of $C$ from $a$ to $b$

*Proof sketch:* Lemma 3 is (1) Lemma 2 is (2). Create $3(d-2)$ paths connecting borders of $Box(u), Box(v), Box(w)$. Recall that $3n^{1/7} \leq d-2$, so we can choose three paths that connect $Box(u), Box(v), Box(w)$ borders. Connect $u, v, w$ to their borders. This gives us $3.1, 3.2, 3.3$.

# How to see Proposition 1



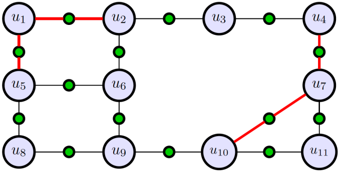
# Connect marked input vertices into paths

Split input $\{0,1\}^{k\times k}$ to $a = \{0,1\}^{k^2-3}$ and $b = (b_u, b_v, b_w)$. ($|a|$ even)

## (Recall) 3.1 and 3.2

- 3.1: $C$ does not use any edge from the external border of $\overline{G_d}$, $\partial(\overline{G_d})$
- 3.2: $C \cap V_d^2 = \{u, v, w\}$

- (3.1) and (3.2) $\implies$ $\exists$ a $a$-covering $\{p_1, ..., p_{|a|/2}\}$ of $V_d^2 \backslash \{u, v, w\}$ that does not intersect $C$



# Using $a$-covering to form affine functions

Fix the values of $a$ and random bits $\implies$ left with $(b_u, b_v, b_w)$ as input

$$\lambda_1 = \bigoplus_{\ell \in V_d} z_\ell \text{ (parity of original vertices)}$$

$$\lambda_2 = \bigoplus_{i=1}^{|a|/2} \bigoplus_{\ell \in p_i \cap V_d^*} z_\ell \text{ (parity of extended vertices in } a\text{-covering)}$$

**The affine functions of $(b_u, b_v, b_w)$**

$$y = \begin{cases} \lambda_1 \oplus \lambda_2, & \text{if } |a| \mod 4 = 0 \\ \lambda_1 \oplus \lambda_2 \oplus 1, & \text{if } |a| \mod 4 = 2 \end{cases}$$

$$y_x = \bigoplus_{\ell \in q_x \cap V_d^*} z_\ell \quad \forall x \in \{u \to v, v \to w, w \to u\}$$

Why are these affine functions of $(b_u, b_v, b_w)$?

# Why $y$ and $y_x$ are affine functions of $(b_u, b_v, b_w)$

**(Recall) 1 and 3.3**

- 1: The lightcones of $x_u, x_v, x_w$ are pairwise disjoint
- 3.3: $q_{v\to w} \cap L(x_u) = \emptyset$, $q_{w\to u} \cap L(x_v) = \emptyset$, $q_{u\to v} \cap L(x_w) = \emptyset$, where $q_{a\to b}$ is the subpath of $C$ from $a$ to $b$

(1) $\implies$ $x_u, x_v, x_w$ do not simultaneously affect any output bit $\implies$ $y, y_x$ are affine in $b_u, b_v, b_w$
(3.3) $\implies$ $y_{u\to v}(b_u, b_v)$, $y_{v\to w}(b_v, b_w)$, $y_{w\to u}(b_w, b_u)$

# Parity results of $NC^0$ measurement outcomes

## (Recall) Theorem 3

For any cycle $C$ of $\overline{G}$, with probability 1, $\bigoplus_{v \in C \cap V^*} z_v = 0$

$$\implies y_{u \to v} \oplus y_{v \to w} \oplus y_{w \to u} = 0$$

## (Recall) Theorem 4

Let $|f|$ be even and $z_V = \bigoplus_{v \in V} z_v$. Then with probability 1,

$$z_V \oplus \bigoplus_{i=1}^{|f|/2} \bigoplus_{v \in p_i \cap V^*} z_v = \begin{cases} 0, & \text{if } |f| \mod 4 = 0 \\ 1, & \text{if } |f| \mod 4 = 2 \end{cases}$$

$$\implies$$

$$\begin{cases} y = 0, & \text{if } (b_u, b_v, b_w) = (0,0,0) \\ y \oplus y_{v \to w} = 1, & \text{if } (b_u, b_v, b_w) = (0,1,1) \\ y \oplus y_{w \to u} = 1, & \text{if } (b_u, b_v, b_w) = (1,0,1) \\ y \oplus y_{u \to v} = 1, & \text{if } (b_u, b_v, b_w) = (1,1,0) \end{cases}$$

# Impossibility of $NC^0$ measurement parity

This is impossible!

## (Recall) Lemma 1

Consider the affine functions

$$q : \{0,1\}^3 \to \{0,1\} \text{ and } q_i : \{0,1\}^2 \to \{0,1\} \text{ for } i \in \{1,2,3\}$$

If $q_1(b_2, b_3) \oplus q_2(b_1, b_3) \oplus q_3(b_1, b_2) = 0$, then one of the following equations does not hold:

$$q(0,0,0) = 0 \tag{5}$$

$$q(0,1,1) \oplus q_1(1,1) = 1 \tag{6}$$

$$q(1,0,1) \oplus q_2(1,1) = 1 \tag{7}$$

$$q(1,1,0) \oplus q_3(1,1) = 1 \tag{8}$$

# What have we shown?

Classical circuit fails for $\geq \frac{1}{8}$ choices of $(b_u, b_v, b_w)$. $|a|$ is even w.p. $\frac{1}{2}$.
For any randomized circuit with random string $r$,

$\implies \sum_{A \in \{0,1\}^{k \times k}} Pr_r[C_d(A) \notin \Lambda_d(A)] \geq \frac{2^{k^2}}{16}$

$\implies$ Average probability $\frac{1}{2^m} \sum_{A \in \{0,1\}^m} Pr_r[C_d(A) \in \Lambda_d(A)] < \frac{15}{16}$

$\implies$ Average probability of success for $NC^0$ circuit $< \frac{15}{16}$

- Global quantum correlations can be realized for all cycles in constant quantum depth
- Sub-logarithmic depth classical circuits cannot create necessary correlations in all long cycles

# Extending the result to average-case hardness

**Theorem 5: Repetition Theorem**

For $m$-input, $n$-output relation $R$, if any depth $\leq c\log_2(m)$ classical circuit $C$ satisfies

$$\frac{1}{2^m}\sum_{x\in\{0,1\}^m} Pr[C(x)\in R(x)] < 1-\alpha$$

then $\forall t \geq 6nm^c + 2$ s.t. any classical $(mt)$-input, $(nt)$-output circuit $C'$ with same bounded depth satisfies

$$\frac{1}{2^{mt}}\sum_{x'\in\{0,1\}^{mt}} Pr[C'(x')\in R^{\times t}(x')] < (1-\alpha)^{t/(6m^c n+2)}$$

In our case, choose $t = (6nm^{1/8}+2)^3$

$\implies \frac{1}{2^{mt}}\sum_{\{0,1\}^{mt}} Pr[\text{success}] < (1-\alpha)^{\sqrt{mt}} \leq \exp\left(-\alpha\sqrt{mt}\right)$

# In conclusion

- No randomized $NC^0$ circuit can solve GSM with average probability $\geq \frac{1}{\exp(\gamma\sqrt{n})}$ for some $\gamma > 0$
- A $QNC^0$ circuit can solve GSM on all inputs with certainty
- Separation for **exponentially small** classical correctness and **simpler** $QNC^0$ algorithm