Nonlocality in Shallow Quantum Circuits

Alexandra Veliche

Northeastern University, Boston, MA

Introduction

Quantum supremacy is expected to drastically change modern computing, but physical implementation is difficult due to nature of qubits.

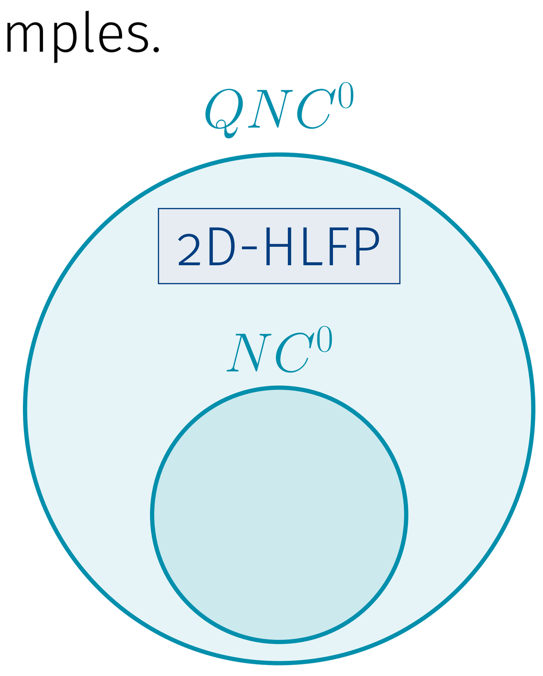
Due to limitations, there is increasing interest in Noisy Intermediate-Scale Quantum technology (50-100 qubits).

In 2017, Bravyi, Gosset, and König publish "Quantum Advantage of Shallow Circuits".

Authors prove quantum circuits are more powerful than classical ones, without complexity theory assumptions. In particular,

$$2D\text{-}HLFP \in QNC^0 \setminus NC^0.$$

We illustrated the importance of the nonlocality property in shallow quantum circuits by proving some of their results for some small examples.



$\mathbf{NC^0}$ = complexity class of all poly-size circuits of $O(1)$ depth with bounded fan-in gates

$\mathbf{QNC^0}$ = quantum analog of NC^0

Hidden Linear Function Problem

Hidden Linear Function Problem (HLFP):

Given: quadratic form $q : \mathbb{F}_2^n \to \mathbb{Z}_4$,

$$q(x) = 2 \sum_{1 \le i < j \le n} A_{ij} x_i x_j + \sum_{k=1}^{n} b_k x_k,$$

where $x_k, A_{ij}, b_k \in \mathbb{F}_2^n$.

Find: $z \in \mathbb{F}_2^n$ such that $q(x) = 2z^T x$, $\forall x \in \mathcal{L}_q$, where $\mathcal{L}_q$ denotes the set

$$\{x \in \mathbb{F}_2^n \mid q(x \oplus y) = q(x) + q(y), \forall y \in \mathbb{F}_2^n\}.$$

2D-HLFP:

Let $G = (V, E)$ denote the $N \times N$ grid graph and $A \in \{0,1\}^{|E|}$ be its adjacency matrix.

Given: quadratic form $q : \mathbb{F}_2^{|V|} \to \mathbb{Z}_4$

$$q(x) = 2 \sum_{(u,v) \in E} x_u x_v + \sum_{v \in V} b_v x_v,$$

where $b \in \{0,1\}^{|V|}$

Find: $z \in \mathbb{F}_2^{|V|}$ such that $q(x) = 2z^T x, \forall x \in \mathcal{L}_q$.

Background

Quantum logic gates used in circuit $\mathcal{Q}_N$:

$$\boxed{H} := \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}, \quad \boxed{S} := \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix},$$

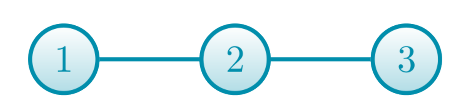
$$\boxed{X} := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \boxed{Y} := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

$$\boxed{Z} := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \boxed{CZ} := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Definition: Let $G = (V, E)$ be a finite simple graph with $|V| = n$ and $|E| = m$. Suppose that a qubit is associated with each vertex of G. The n-qubit graph state of G is

$$|\phi_G\rangle := \left(\prod_{(u,v) \in E} CZ_{uv} \right) H^{\otimes n} |0^n\rangle.$$

Example:



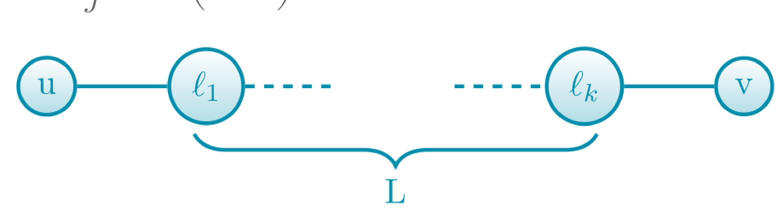
$V = \{1,2,3\}, E = \{(1,2),(2,3),(3,2),(2,1)\}$

$$|\phi_G\rangle = CZ_{12} CZ_{23} H^{\otimes 3} |0^3\rangle = \tfrac{1}{\sqrt{8}}(|000\rangle + |001\rangle + \dots + |111\rangle).$$

Claim: For finite simple graph $G = (V, E)$, $|\phi_G\rangle$ is a stabilizer state for the stabilizer group generated by the operators

$$g_v := X_v \left(\prod_{(u,v) \in E} Z_u \right), \forall\, v \in V.$$

Definition: Let $z \in \{0,1\}^*$. For a bit z_j of z, define $m_j := (-1)^{z_j}$. Describe G and L by



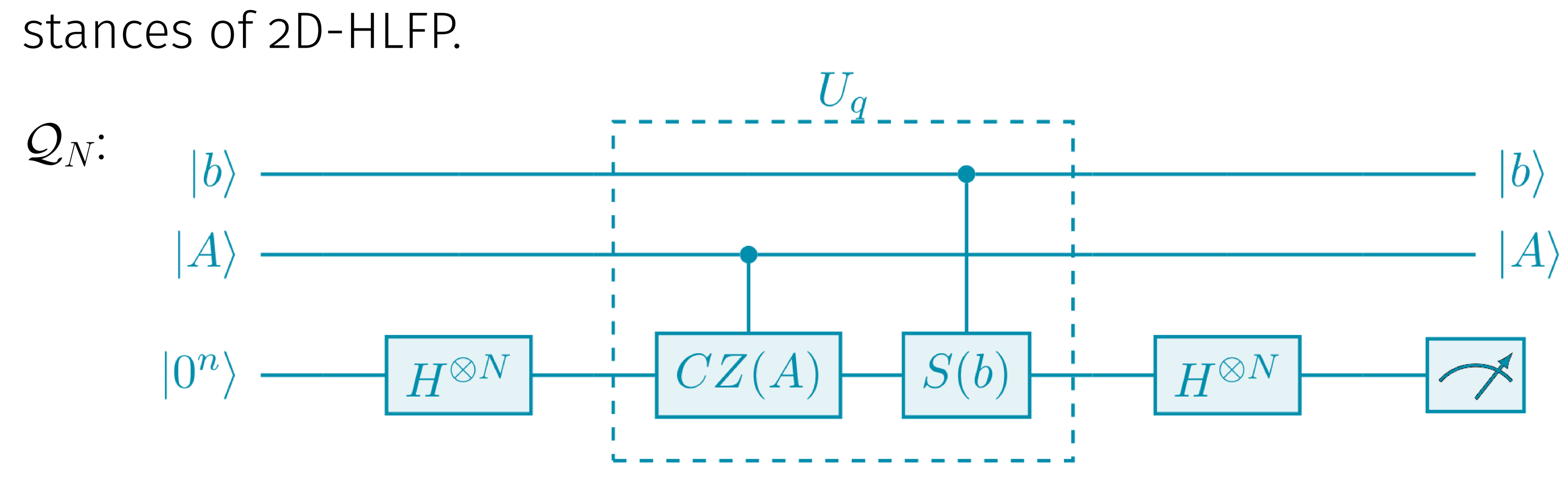
We define L_{odd} and similarly

$$L_{even} := \{\ell \in L \mid \delta(\ell, u) \equiv 0 \,(mod\, 2) \equiv \delta(\ell, v)\}.$$

Also define $m_L := \prod_{j \in L_{odd}} m_j$.

Quantum Circuit for 2D-HLFP

Theorem: For every $N \ge 2$, there exists a quantum circuit $\mathcal{Q}_N$ of depth $d = O(1)$ which deterministically solves size-N instances of 2D-HLFP.

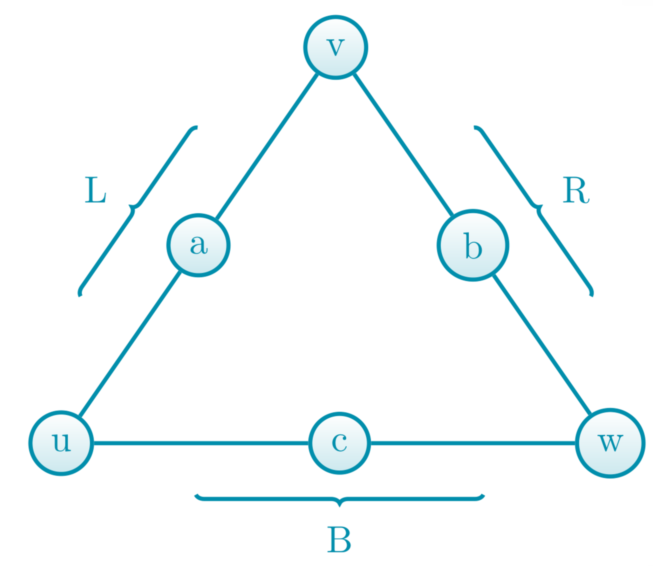


$$CZ(A) := \prod_{1 \le i < j \le N} CZ_{ij}^{A_{ij}} \text{ and } S(b) := \bigotimes_{j=1}^{N} S_j^{b_j}.$$

Nonlocality Property

Nonlocality: a form of correlation present in the measurement statistics of entangled quantum states that cannot be reproduced by local hidden variable models.

Example: Let G describe the graph below



Let $b := b_u b_v b_w \in \{0,1\}^3$ and define

$$\mathcal{T}(b) := \{z \in \{0,1\}^m \mid \langle z | H^{\otimes m} S_u^{b_u} S_v^{b_v} S_w^{b_w} |\phi_G\rangle \neq 0\}.$$

Claim: Let $b = b_u b_v b_w \in \{0,1\}^3$ and $z \in \mathcal{T}(b)$. Then $m_R m_B m_L = 1$. If $b_u \oplus b_v \oplus b_w = 0$, then $i^{b_u + b_v + b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = 1$.

Lemma: The stabilizers of $|\phi_G\rangle$ are

$$X_u X_v X_w, -X_u Y_v Y_w X_a X_c, -Y_u X_v Y_w X_a X_b,$$
$$\text{and } -Y_u Y_v X_w X_b X_c.$$

Measurements on classical local circuits cannot simultaneously satisfy these nonlocality identities!

Acknowledgements

I would like to thank the following people for their guidance and support in this project:

Advisor & Consultant: Professor Christopher King

Secondary Advisor: Professor Christopher Beasley

Faculty Coordinator: Professor Anthony Iarrobino

Sponsors: NCUWM, Northeastern University

References

[1] Bravyi, S., Gosset, D., & König, R. (2018). Quantum Advantage with Shallow Circuits. *Science*. *362*(6412), 308-311. Retrieved from: `https://arxiv.org/pdf/1704.00690.pdf`.

[2] (2019). *Discussions with Prof. Christopher King*.

[3] Preskill, J. (2018). Quantum Computing in the NISQ Era and Beyond. *Quantum*. *2*(79). Retrieved from: `https://arxiv.org/pdf/1801.00862.pdf`.

[4] Corner image retrieved from: `https://www.hiclipart.com/`.