Nonlocality in Shallow Quantum Circuits

Junior/Senior Honours Thesis

(Math 4971)

Alexandra Veliche

December 5, 2019

Faculty Consultant: Professor Christopher King

Abstract: In this paper, I illustrate the nonlocality properties that give shallow quantum circuits an advantage over their classical counterparts. To do this, I focus on a few small examples of the main results presented in the paper ”Quantum Advantage of Shallow Circuits” by Sergey Bravyi, David Gosset, Robert König. I prove some of their results for these examples and discuss their connection to the 2D-Hidden Linear Function Problem, the problem they used to separate the classes NC^0 from QNC^0. My contribution consists of the detailed proofs of these small examples and an introductory exposition of the key ideas in the paper.

Keywords: shallow quantum circuits, Noisy Intermediate-Scale Quantum technology, nonlocality, Hidden Linear Function Problem

Acknowledgements: I would like to thank my advisor, Professor Christopher King, for his guidance and patience throughout this research project. I would also like to thank Professor Christopher Beasley for his guidance in exploring related topics in preparation for this project.

Contents

1 Introduction

In the past few decades, there has been a significant amount of interest and research in the field of quantum computing. It has been shown that quantum computers are theoretically more powerful than their classical counterparts, but the physical implementation of these quantum computers is difficult due to the nature of qubits [9]. If sufficiently-powerful quantum computers are ever constructed, this potential running-time advantage, known as “quantum supremacy” [8], is expected to heavily impact modern computing, and hence modern privacy and security.

A famous example is the quantum algorithm developed by Peter Shor in 1995, which can factor a given number with a running time polynomial in the size of the number being factored [9]. Shor’s algorithm consists of two parts: a classical algorithm that reduces the problem of finding the non-trivial divisors of a given number N to finding the order of a particular number modulo N, and a quantum subroutine that finds the order of that element using the quantum Fourier transform and arrangement of quantum logic gates in a specific circuit [6]. The problem of factoring a random integer is considered to be infeasible for classical computers, and no classical algorithm for polynomial-time factoring is believed to exist. This is because the factoring problem lies in the classical complexity class of decision problems solvable in nondeterministic polynomial time (NP), which contains the class of polynomial-time problems (P), so finding a classical polynomial-time algorithm would partially solve the Millennium Prize problem of “P =? NP” [3]. Because several commonly-used cryptosystems, such as RSA and variants of Elliptic-Curve Cryptography (ECC), rely on the difficulty of this problem, Shor’s result poses a threat to public-key cryptography as we know it [4]. As a result, there has been increasing interest in post-quantum cryptography, which involves cryptographic schemes resistant to quantum attacks; these include lattice-based GGH and NTRU-Encrypt [3]. Despite this threat, it is believed that a quantum computer operating with thousands of qubits and billions of logic gates would be necessary to accurately perform these kinds of computations. This large number of qubits and gates would be required to compensate for errors produced as a result of ambient noise that would interfere with the qubits’ behavior [2]. Without error-correction capabilities, a quantum computation can only run for constant time before the qubits decohere and entropy accumulates. [2]

For the time being, there has been increasing interest in quantum computers with far fewer qubits – about 50-100 qubits – which are expected to be available in the next few years [7]. This technology is known as Noisy Intermediate-Scale Quantum (NISQ) technology and is believed to be capable of performing computations that would surpass the capabilities of modern classical computers [7]. This past October, Google unveiled their new 53-qubit quantum computer, which they claim to have solved an obscure problem in a few minutes, that would otherwise have taken a classical computer thousands of years [8]. While the demonstration does not have any practical application [8], the development is a first step in the direction of producing quantum computers for practical purposes.

As part of this effort, Bravyi, Gosset, and König wrote a paper called "Quantum Advantage of Shallow Circuits", in which they show that constant-depth quantum circuits are more powerful than their classical counterparts [2]. They examine computations performed by Shallow Quantum Circuits (SQC) – constant-depth quantum circuits executed by quantum parallel algorithms running in constant time. Because NISQ technology may not have error-correction capabilities by definition, parallelization and circuit depth are important factors to consider when designing quantum algorithms for these computers. This is in order to optimize the efficiency of the computations being performed in the time-frame before the qubits decohere.

NC^0 denotes the complexity class of all decision problems solvable by a classical circuit of polynomial size, constant depth, and bounded fan-in [11]. The quantum analog to this class is QNC^0. In their paper, Bravyi, Gosset, and König focus on a particular case of the Hidden Linear Function Problem (HLFP, defined in section 1.3). They demonstrate that this problem can be solved with certainty by a quantum circuit that satisfies the constraints of the QNC^0 class. Furthermore, they show that no classical probabilistic circuit in the class NC^0 can solve the problem with a success probability of greater than $\frac{7}{8}$ [2]. More specifically, any classical probabilistic circuit with fan-in bounded above by K which solves all instances of the 2D-HLFP of size N with a success probability greater than $\frac{7}{8}$ would require a depth of at least $\frac{\log(N)}{8\log(K)}$ [2]. In other words, they show that HLFP is in the complexity class QNC^0 but not in NC^0. It is particularly remarkable that they prove this result unconditionally, without complexity theory assumptions.

One of the special properties of quantum circuits that gives them this advantage in solving the HLFP is the nonlocality constraint presented in s section 5. In this paper, we give detailed proofs for some of the results presented in the original paper for some small examples (see Examples 2.1 and 5.2). This serves to illustrate the significance of nonlocality in quantum shallow circuits.

2 Preliminaries

In this section, we define the terminology used throughout the paper. Recall that a qubit exists in a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$, so it can be represented by a length-2 vector. The states $|0\rangle, |1\rangle$ are known as the *standard* or *computational* basis states of a qubit. Some of the basic gates that act on single qubits are represented by the following set of matrices over $\mathbb{C}$:

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

$$\textit{Pauli X-gate: } X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \textit{Pauli Y-gate: } Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \textit{Pauli Z-gate: } Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

We remark that the standard basis states $|0\rangle$ and $|1\rangle$ correspond to measuring a qubit in the Z-basis, since these are the eigenvectors of Z with eigenvalues ± 1 [5]. Qubit states can also be measured in bases other than the standard basis. For example, a qubit with some state

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be measured in the X-basis by mapping the original basis states to the eigenvectors of X: $|0\rangle \mapsto |+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \mapsto |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then the state can be rewritten as $|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle$ for some $\alpha', \beta' \in \mathbb{C}$.

The *controlled-Z* gate acts on two qubits and is represented by a matrix $CZ \in \mathbb{C}^{4\times 4}$. It can be expressed in terms of the Pauli gates as: $CZ := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$.

We present the following set of observations about the Pauli gates and CZ gate that will be referred to throughout the remainder of this paper:

1. Gates that do not affect the same qubits commute.
2. The Pauli gates X, Y, Z are involutory and anti-commutative.
3. $XY = iZ$, $YZ = iX$, and $ZX = iY$.
4. $X_i|\psi\rangle = |\psi\rangle$, where $|\psi\rangle$ is the uniform superposition of basis states.
5. $CZ_{ij} = CZ_{ji}$.
6. $Z_jCZ_{ij} = CZ_{ij}Z_j$ for all $i, j \in V$.
7. $X_iCZ_{ij} = Z_jCZ_{ij}X_i$ for all $i, j \in V$.
8. $X_jCZ_{ij} = Z_iCZ_{ij}X_j$ for all $i, j \in V$.
9. $SY = XS$.

Definition 2.1. 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. Then the n-qubit *graph state* of G is given by

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

Recall that $H^{\otimes n}$ denotes n Hadamard gates applied in parallel to $|0^n\rangle$, the n qubits initialized to $|0\rangle$. This serves to entangle the qubits. We clarify that in the product of CZ_{uv} gates, only one edge (u, v) for every pair of vertices u and v is represented (even if G is an undirected graph).

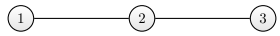
This graph state has special properties that are leveraged to obtain the results of the Bravyi-Gosset-König paper. In particular, the graph state has a clear set of *stabilizer states* - states that keep the graph state invariant when operating on it. The following claim explicitly describes the group of stabilizer states for the graph state:

Claim 2.1. *Let $G = (V, E)$ be a finite simple graph. Then $|\phi_G\rangle$ is a stabilizer state for the stabilizer group generated by the operators g_v, for all $v \in V$, given by*

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

To see why this is true, consider the following example:

Example 2.1. Consider the line graph $G = (V, E)$ represented in the diagram below, where $V = \{1, 2, 3\}$ and $E = \{(1,2), (2,3), (3,2), (2,1)\}$.



By definition, the graph state for this graph is $|\phi_G\rangle = CZ_{12}CZ_{23}H^{\otimes 3}|0^3\rangle$. This can be explicitly expressed in the following manner:

Let $|\psi\rangle := H^{\otimes 3}|0^3\rangle$ denote the state produced by applying the Hadamard gates on the initialized qubits. By definition of the Hadamard gate, this can be written as

$$|\psi\rangle := H^{\otimes 3}|0^3\rangle = \frac{1}{\sqrt{2^3}} \sum_{b_i=0}^{1} b_1 b_2 b_3 = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle).$$

Recall that the gate CZ_{ij} only affects the qubits at vertices i and j and flips the sign of a qubit state if both of these qubits are in the state 1. Applying the gates CZ_{12} and then CZ_{23}, we obtain

$$\begin{aligned} CZ_{23}|\psi\rangle &= \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle) \\ CZ_{12}CZ_{23}|\psi\rangle &= \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle + |111\rangle) = |\phi_G\rangle \end{aligned}$$

Now we prove the claim above for this particular graph:

Claim 2.2. *$|\phi_G\rangle$ is a stabilizer state with stabilizer group generated by*

$$g_1 = X_1 Z_2, \; g_2 = X_2 Z_1 Z_3, \; \text{and } g_3 = X_3 Z_2.$$

Proof: We show that (i) $g_v|\phi_G\rangle = |\phi_G\rangle$ for all $v \in V$, and (ii) any element in the group generated by the g_v is a stabilizer of $|\phi_G\rangle$.

(i) We show that g_1, g_2, and g_3 defined above are stabilizers of the graph state. For clarity, we underline the product of gates being rewritten in each step and reference the property used.

$$\begin{aligned} g_1|\phi_G\rangle &= \underline{X_1}Z_2CZ_{12}CZ_23|\psi\rangle, \text{ by 1} \\ &= Z_2\underline{X_1CZ_{12}}CZ_{23}|\psi\rangle, \text{ by 7} \\ &= \underline{Z_2Z_2}CZ_{12}X_1CZ_{23}|\psi\rangle, \text{ by 2} \\ &= CZ_{12}\underline{X_1CZ_{23}}|\psi\rangle, \text{ by 1} \\ &= CZ_{12}CZ_{23}\underline{X_1|\psi\rangle}, \text{ by 4} \\ &= CZ_{12}CZ_{23}|\psi\rangle = |\phi_G\rangle \end{aligned}$$

$$\begin{aligned} g_2|\phi_G\rangle &= \underline{X_2Z_1Z_3}CZ_{12}CZ_{23}|\psi\rangle, \text{ by 1} \\ &= Z_3Z_1\underline{X_2CZ_{12}}CZ_{23}|\psi\rangle, \text{by 8} \\ &= Z_3\underline{Z_1Z_1}CZ_{12}X_2CZ_{23}|\psi\rangle, \text{ by 2} \\ &= Z_3CZ_{12}\underline{X_2CZ_{23}}|\psi\rangle, \text{ by 7} \\ &= Z_3\underline{CZ_{12}Z_3}CZ_{23}X_2|\psi\rangle, \text{ by 1} \\ &= \underline{Z_3Z_3}CZ_{12}CZ_{23}X_2|\psi\rangle, \text{ by 2} \\ &= CZ_{12}CZ_{23}\underline{X_2|\psi\rangle}, \text{ by 4} \\ &= CZ_{12}CZ_{23}|\psi\rangle = |\phi_G\rangle \end{aligned}$$

$$
\begin{aligned}
g_3|\phi_G\rangle &= \underline{X_3}Z_2CZ_{12}CZ_{23}|\psi\rangle, \text{ by 1} \\
&= \underline{Z_2CZ_{12}}X_3CZ_{23}|\psi\rangle, \text{ by 6} \\
&= CZ_{12}Z_2\underline{X_3CZ_{23}}|\psi\rangle, \text{ by 8} \\
&= CZ_{12}\underline{Z_2Z_2}CZ_{23}X_3|\psi\rangle, \text{ by 2} \\
&= CZ_{12}CZ_{23}\underline{X_3|\psi\rangle}, \text{ by 4} \\
&= CZ_{12}CZ_{23}|\psi\rangle = |\phi_G\rangle
\end{aligned}
$$

Hence $g_1|\phi_G\rangle = |\phi_G\rangle, g_2|\phi_G\rangle = |\phi_G\rangle$, and $g_3|\phi_G\rangle = |\phi_G\rangle$.

(ii) Let $g_{i_1}...g_{i_k} \in \langle g_1, g_2, g_3\rangle$ be an element in the group generated by the stabilizers above, where $i_j \in \{1, 2, 3\}$. Since each g_{i_j} leaves $|\phi_G\rangle$ invariant, it follows that the product composed of these stabilizers leaves the graph state invariant. Hence, any element in $\langle g_1, g_2, g_3\rangle$ is a stabilizer of $|\phi_G\rangle$. ■

Definition 2.2. Let $z \in \{0,1\}^*$ be a bit-string. For a bit z_j of z, define $m_j := (-1)^{z_j}$. Let G be a line graph with end-vertices u and v, and L be the set of vertices that lie between u and v. Then

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

denotes the set of vertices at an even distance from both u and v. Similarly, denote the vertices at an odd distance by L_{odd}. For this L, define $m_L := \prod_{j\in L_{odd}} m_j$.

We note that from this point onward, unless explicitly said otherwise, addition expressed with "+" represents addition modulo 4, while "⊕" represents the usual addition modulo 2.

3 Hidden Linear Function Problem

In their paper, Bravyi, Gosset, and König examine a specific search problem and show that a specific case of this particular problem can be solved with certainty by a quantum circuit with constant depth. They also show that for any classical circuit there is a problem of this type whose solution with probability greater than 7/8 requires a depth logarithmic in the size of the instance of the problem. The problem of focus is the Hidden Linear Function Problem defined below [2]:

Definition 3.1. The *Hidden Linear Function Problem (HLFP)* is a search problem stated as follows: given a quadratic form $q : \mathbb{F}_2^n \to \mathbb{Z}_4$ defined by

$$q(x) = 2 \sum_{1\leq a<b\leq n} A_{\alpha,\beta}x_\alpha x_\beta + \sum_{i=1}^{n} b_i x_i,$$

where $x_1, ...x_n \in \{0, 1\}$ are binary variables and $A_{\alpha,\beta} \in \{0, 1\}, b_i \in \{0, 1\}$ are specified by a matrix A and vector b, find a binary vector $z \in \{0, 1\}^n$ such that $q(x) = 2z^T x$ for all $x \in \mathcal{L}_q$, where

$$\mathcal{L}_q := \{x \in \mathbb{F}_2^n \mid q(x \oplus y) = q(x) + q(y) \ (mod\ 4) \text{ for all } y \in \mathbb{F}_2^n\}.$$

Bravyi, Gosset, and König show that the restriction of the quadratic form $q(x)$ to the set $\mathcal{L}_q$ is always a linear form, meaning that there exists a vector $z \in \mathbb{F}_2^n$ that satisfies $q(x) = 2z^T x$. Hence the HLFP asks for a solution to this problem, for the given $q(x)$ specified by A and b. The $2D$-Hidden Linear Function is a particular case of the HLFP, in which the matrix A has a specific structure:

Definition 3.2. The *2D Hidden Linear Function Problem (2D-HLFP)* is a special case of the HLFP, where the inputs have a specific structure: Let $G = (V, E)$ be the graph describing an $N \times N$ grid. Define $A \in \{0,1\}^{|E|}$ to be the $N^2 \times N^2$ adjacency matrix of G, where $A_{(u,v)} = 0$ unless $(u, v) \in E$, and $b \in \{0,1\}^{|V|}$. Given a quadratic form q specified by A and b as

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

find a vector $z \in \{0,1\}^{|V|}$ such that $q(x) = 2z^T x$ for all $x \in \mathcal{L}_q$. We call this a *size-N instance* of the 2D-HLFP.

Note that here the number of input bits is $|V| + |E| = N^2 + 2N(N-1) = 3N^2 - 2N$.

The following result formally states the significance of this problem in showing the separation between classical and quantum shallow circuits (which we state without proof):

Theorem 3.1. *For every instance $N \geq 2$, there exists a quantum circuit $\mathcal{Q}_N$ of depth $d = O(1)$ which deterministically solves size-N instances of the 2D-HLFP.*

This quantum circuit $\mathcal{Q}_N$ is presented in the following section.

4 Quantum Circuit for HLFP

In this section we present the quantum circuit that deterministically solves instances of the 2D-HLFP for a given size N[2]. In the circuit below, the controlled gates determined by the inputs of the HLFP A and b are the following:

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

The circuit below deterministically solves all size-N instances of the 2D-HLFP [2]:

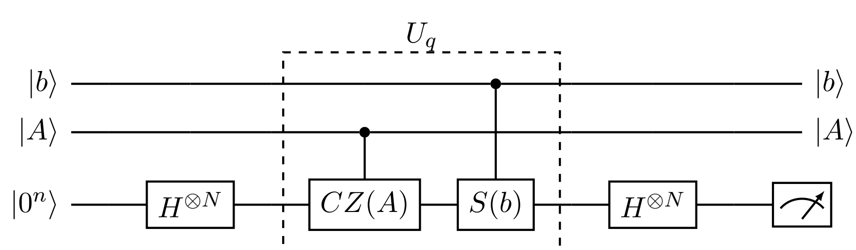


Figure 1: Quantum Circuit for size-N instance of 2D-HLFP

The $CZ(A)$ and $S(B)$ gates above can be expressed as constant-depth quantum circuits composed of the gates presented in section 2. Since there are a fixed number of gates in this circuit, it follows that the depth remains constant for any instance of size N [2].

We make the following remark about the run-time of this circuit: Since any set of gates that operate on distinct sets of qubits do not interfere with each other, these gates can be operated in parallel simultaneously in the circuit. This simultaneous operation can be considered as one step in the computation. Hence, the run-time of such a step is given by the run-time for a single gate, which is fixed. In this way, the gates in the circuit can be partitioned into a small number of disjoint sets such that the gates in each set can be operated simultaneously. Because the number of such sets is independent of the size of the input N, the total run-time does not depend on N. Thus, this circuit runs in constant time.

5 Nonlocality

One of the properties of qubits that differentiate them from classical bits is *quantum nonlocality*. This is a phenomenon in which measurement results of entangled quantum states cannot be reproduced by completely local functions where every output bit depends only on one input bit and some randomness. With this property, qubits in the output may depend on multiple input qubits that may be physically distant (even light-years away) from each other.

A fundamental example of the way nonlocality produces the separation between the capabilities of quantum and classical circuits is given by the *Greenberger–Horne–Zeilinger state* below [2]:

Example 5.1. Consider the 3-qubit state

$$|GHZ\rangle := \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

A set of stabilizers for this state is $P := \{X_1X_2X_3, -X_1Y_2Y_3, -Y_1X_2Y_3, -Y_1Y_2X_3\}$. (This can easily be shown using our set of observations as in the proof of Claim 2.2 above).

Now let $b = b_1b_2b_3 \in \{0,1\}^3$ be a bit-string and suppose that each qubit j of $|GHZ\rangle$ is measured in the X-basis if $b_j = 0$ or the Y-basis if $b_j = 1$, giving the measurement outcomes $m \in \{-1,1\}^3$. Then using the four stabilizers in P, we see that the measurement statistics satisfy the following constraint:

$$\text{If } b_1 \oplus b_2 \oplus b_3 = 0, \text{ then } i^{b_1+b_2+b_3} m_1m_2m_3 = 1.$$

Each of the four cases ($b = 000, 011, 101, 110$) of this condition cannot be solved by any local classical measurement, however, where each m_j depends on just one of the bits b_k. [10] □

Now we illustrate the geometric nonlocality properties of single-qubit measurements on the 1-dimensional graph state corresponding to an even-length cycle graph [2]. Due to the peculiar properties of qubits, the measurement outcomes of a circuit with this property cannot be simulated by shallow classical circuits that are 1-dimensionally geometrically local [2].

The key idea behind the cycle graph below is the following: fix any three vertices in the quantum circuit, and consider the triangle graph they determine. In examining the way these qubits affect each other's states, we see that these satisfy a certain constraint not necessarily present in a classical circuit. Using the following example, we illustrate the concept of quantum nonlocality and state results that describe the significance of nonlocality in proving the advantage of quantum shallow circuits over classical ones:

Example 5.2. Let $G = (V, E)$ be the cycle graph represented by the diagram below, with $m := |V| = 6 = |E|$. We let u, v, and w denote the vertices that are pair-wise at an even distance from each other, and label the other vertices by a, b, and c. This graph can be thought of as a triangle determined by the vertices u, v, and w. Denote the sets of vertices to the right, left, and bottom of the triangle by R, L, and B, respectively. Notice that in this particular case, there are only odd vertices (a, b, c) and no even vertices.

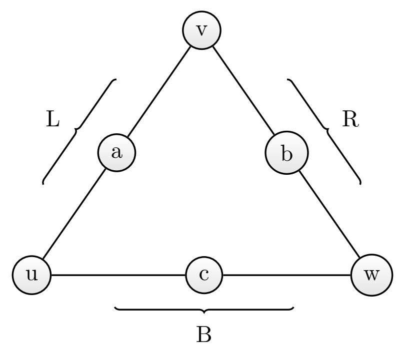


Figure 2: 6-Vertex Cycle Graph

The graph state corresponding to this graph is given by

$$|\phi_G\rangle = CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}H^{\otimes 6}|0^6\rangle.$$

□

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

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

to be the set of possible measurements of the qubits arranged in this graph formation. Here the qubits in the graph state are measured in the X-basis (where the columns of X determine the basis vectors $|0\rangle$ and $|1\rangle$) and u, v, w are measured in the X- or Y-basis according to b: if $b_i = 0$, then qubit i is measured in the X-basis, otherwise it is measured in the Y-basis.

One of the manifestations of quantum nonlocality is the constraint given in the claim below from the Bravyi-Gosset-König paper. Informally, this states that for any length-3 string b and measurement z, the sum of the measurements of the bits of z corresponding to the set $R \cup B \cup L$ must be even. In addition to this, if the string b has an even Hamming weight, a stronger constraint holds. We explicitly prove the general claim for the case where G is the graph in Figure 2:

Claim 5.1. *Let $b = b_u b_v b_w \in \{0,1\}^3$ and $z \in \mathcal{T}(b)$. Then $m_R m_B m_L = 1$.*
Moreover, if $b_u \oplus b_v \oplus b_w = 0$, then $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = 1$.

Proof: (for Example 5.2) We prove both parts of the claim as follows:

(i) *To show:* $m_R m_B m_L = 1$.

Let $Odds := R_{odd} \cup L_{odd} \cup B_{odd}$. For this graph G, the only vertices are $\{a, b, c\}$. Define $X(Odd) := \prod_{j \in Odd} X_j$ and $g(Odd) := \prod_{j \in Odd} g_j$. In this case, $X(Odd) = X_a X_b X_c$ and

$$\begin{aligned} g(Odd) = g_a g_b g_c &= (X_a Z_v Z_w)(X_b Z_u Z_v)(X_c Z_w Z_u), \text{ by definition} \\ &= X_a X_b X_c Z_u^2 Z_v^2 Z_w^2, \text{ by properties of Pauli gates} \\ &= X_a X_b X_c. \end{aligned}$$

Since the g_j are stabilizers of the graph state $|\phi_G\rangle$, it follows that $g(Odd) = X_a X_b X_c$ is a stabilizer for $|\phi_G\rangle$. Then, $X_a X_b X_c |\phi_G\rangle = |\phi_G\rangle$. Now consider the measurement $\langle z| H^{\otimes 6} X_a X_b X_c |\phi_G\rangle$. Since the Hadamard gate produces a measurement in the X-basis and by the properties of the X gate, this can be rewritten as follows:

$$\begin{aligned} \langle z| H^{\otimes 6} X_a X_b X_c |\phi_G\rangle &= \langle z_x | X_a X_b X_c |\phi_G\rangle \\ &= (-1)^{z_a + z_b + z_c} \langle z_x | \phi_G \rangle \\ &= (-1)^{z_a + z_b + z_c} \langle z | H^{\otimes 6} | \phi_G \rangle \end{aligned}$$

By the result above, $\langle z| H^{\otimes 6} X_a X_b X_c |\phi_G\rangle = \langle z | H^{\otimes 6} | \phi_G \rangle$, so it follows that $(-1)^{z_a+z_b+z_c} = 1$. Rewriting, we obtain

$$(-1)^{z_a+z_b+z_c} = (-1)^{z_a}(-1)^{z_b}(-1)^{z_c} = m_a m_b m_c = m_L m_B m_R = 1.$$

(ii) *To show:* If $b_u \oplus b_v \oplus b_w = 0$, then $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = 1$.

For this part, we make use of some of the stabilizer states of the graph G. In particular, we rely on the following lemma:

Lemma 5.1. *The following operators are stabilizers of the graph state $|\phi_G\rangle$:*

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

Proof of Lemma: (see Appendix) □

If $b = b_u \oplus b_v \oplus b_w = 0$, then there are four cases to consider: $b = 000, 011, 101,$ or 110. For each of these cases, we consider the properties of the measurement of $z \in \mathcal{T}(b)$. We use the lemma above to derive conditions from the stabilizers that correspond to each of these cases, similar to part (i).

$\underline{b = 000}$: In this case, the qubits in positions u, v, and w are all measured in the X-basis. By definition, $S_u^{b_u} S_v^{b_v} S_w^{b_w} = 1$. Hence, we can use the stabilizer $X_u X_v X_w$ to rewrite the measurement of z:

$$\langle z|H^{\otimes 6} X_u X_v X_w|\phi_G\rangle = (-1)^{z_u z_v z_w}\langle z|H^{\otimes 6}|\phi_G\rangle \text{ by } X \text{ gate definition.}$$

By the lemma, $\langle z|H^{\otimes 6} X_u X_v X_w|\phi_G\rangle = \langle z|H^{\otimes 6}|\phi_G\rangle$, so it follows that $(-1)^{z_u z_v z_w} = 1$. Rewriting, we obtain:

$$(-1)^{z_u z_v z_w} = (-1)^{z_u}(-1)^{z_v}(-1)^{z_w} = m_u m_v m_w = 1.$$

Thus, $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = i^0 m_u m_v m_w = 1$.

$\underline{b = 011}$: In this case, the qubits in position u is measured in the X-basis and v and w are measured in the Y-basis. By definition, $S_u^{b_u} S_v^{b_v} S_w^{b_w} = S_v S_w$. Hence, we use the stabilizer $-X_u Y_v Y_w X_a X_c$ to rewrite the measurement of z:

$$\begin{aligned}
\langle z|H^{\otimes 6} S_v S_w(-X_u Y_v Y_w X_a X_c)|\phi_G\rangle &= -\langle z|H^{\otimes 6} X_u(S_v Y_v)(S_w Y_w) X_a X_c|\phi_G\rangle \\
&= -\langle z|H^{\otimes 6} X_u(X_v S_v)(X_w S_w) X_a X_c|\phi_G\rangle, \text{ by 7} \\
&= -\langle z|H^{\otimes 6} X_u X_v X_w X_a X_c S_v S_w|\phi_G\rangle, \text{ by 1} \\
&= -(-1)^{z_u+z_v+z_w+z_a+z_c}\langle z|H^{\otimes 6} S_v S_w|\phi_G\rangle.
\end{aligned}$$

By the lemma, $\langle z|H^{\otimes 6} S_v S_w(-X_u Y_v Y_w X_a X_c)|\phi_G\rangle = \langle z|H^{\otimes 6} S_v S_w|\phi_G\rangle$, so it follows that $-(-1)^{z_u+z_v+z_w+z_a+z_c} = 1$. Rewriting, we obtain:

$$\begin{aligned}
(-1)^{z_u+z_v+z_w+z_a+z_c} &= (-1)^{z_u}(-1)^{z_v}(-1)^{z_w}(-1)^{z_a}(-1)^{z_c} \\
&= m_u m_v m_w m_a m_c = m_u m_v m_w m_L m_B = -1.
\end{aligned}$$

Thus, $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = i^2 m_u m_v m_w m_L m_B = (-1)(-1) = 1$.

Since the cases $b = 101$ and $b = 110$ are almost identical to the case $b = 011$, we omit the details for these cases here (see Appendix for details).

Hence condition (ii) holds for all b that satisfy the hypothesis. ∎

6 Conclusion

In the previous sections, we illustrate how the quantum circuit with its corresponding graph state has certain properties that are not necessarily found in classical circuits [2]. We referred to the GHZ state as a key example of this and later examined the role of the graph state in showing that quantum circuits must satisfy certain constraints as a result of nonlocality. In the original paper, the authors use the nonlocality constraints of Claim 5.1 to show that the input and output bits of a classical circuit are not necessarily correlated in the same way.

The goal of the classical circuit analysis is to find a cycle in the classical circuit similar to that in Example 5.2, for which the identities in Claim 5.1 cannot be satisfied with certainty. In the $N \times N$ grid corresponding to the classical circuit that solves the 2D-HLFP, three vertices u, v, w can be found that do not exhibit the nonlocality properties. The cycle graph determined by these three vertices determine the matrix A and vector b that define a subset of instances of the 2D-HLFP [2]. This is the key idea to showing that classical circuits are not able to solve the 2D-HLFP with the certainty and constant-depth of their quantum counterparts.

7 Appendix

In this section we include the last two cases of the proof of Claim 5.1 for completeness. We also give a detailed proof of Lemma 5.1 used to prove part (ii) of Claim 5.1 for Example 5.2.

Proof of Claim 5.1 (cases b=101 and b=110):

$\underline{b = 101}$: In this case, the qubits in positions u and w are measured in the Y-basis and v is measured in the X-basis. By definition, $S_u^{b_u} S_v^{b_v} S_w^{b_w} = S_u S_w$. Hence, we use the stabilizer $-Y_u X_v Y_w X_a X_b$ to rewrite the measurement of z:

$$\begin{aligned}\langle z|H^{\otimes 6} S_u S_w(-Y_u X_v Y_w X_a X_b)|\phi_G\rangle &= -\langle z|H^{\otimes 6} X_v (S_u Y_u)(S_w Y_w) X_a X_b|\phi_G\rangle, \text{ by property 1} \\ &= -\langle z|H^{\otimes 6} X_v (X_u S_u)(X_w S_w) X_a X_b|\phi_G\rangle, \text{ by property 7} \\ &= -\langle z|H^{\otimes 6} X_u X_v X_w X_a X_b S_u S_w|\phi_G\rangle, \text{ by property 1} \\ &= -(-1)^{z_u+z_v+z_w+z_a+z_b}\langle z|H^{\otimes 6} S_u S_w|\phi_G\rangle, \text{ by } X \text{ gate definition.}\end{aligned}$$

By the lemma, $\langle z|H^{\otimes 6} S_u S_w(-Y_u X_v Y_w X_a X_b)|\phi_G\rangle = \langle z|H^{\otimes 6} S_u S_w|\phi_G\rangle$, so it follows that $-(-1)^{z_u+z_v+z_w+z_a+z_b} = 1$. Rewriting, we obtain:

$$\begin{aligned}(-1)^{z_u+z_v+z_w+z_a+z_b} &= (-1)^{z_u}(-1)^{z_v}(-1)^{z_w}(-1)^{z_a}(-1)^{z_b} \\ &= m_u m_v m_w m_a m_b = m_u m_v m_w m_L m_R = -1.\end{aligned}$$

Thus, $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = i^2 m_u m_v m_w m_R m_L = (-1)(-1) = 1.$

$\underline{b = 110}$: In this case, the qubits in positions u and v are measured in the Y-basis and w is measured in the X-basis. By definition, $S_u^{b_u} S_v^{b_v} S_w^{b_w} = S_u S_v$. Hence, we use the stabilizer $-Y_u Y_v X_w X_b X_c$ to rewrite the measurement of z:

$$\begin{aligned}\langle z|H^{\otimes 6} S_u S_v(-Y_u Y_v X_w X_b X_c)|\phi_G\rangle &= -\langle z|H^{\otimes 6} (S_u Y_u)(S_v Y_v) X_w X_b X_c|\phi_G\rangle \\ &= -\langle z|H^{\otimes 6} (X_u S_u)(X_v S_v) X_w X_b X_c|\phi_G\rangle \text{ by property 7} \\ &= -\langle z|H^{\otimes 6} X_u X_v X_w X_b X_c S_u S_v|\phi_G\rangle \text{ by property 1} \\ &= -(-1)^{z_u+z_v+z_w+z_b+z_c}\langle z|H^{\otimes 6} S_u S_v|\phi_G\rangle \text{ by } X \text{ gate definition.}\end{aligned}$$

By the lemma, $\langle z|H^{\otimes 6} S_u S_v(-Y_u Y_v X_w X_b X_c)|\phi_G\rangle = \langle z|H^{\otimes 6} S_u S_v|\phi_G\rangle$, so it follows that $-(-1)^{z_u+z_v+z_w+z_b+z_c} = 1$. Rewriting, we obtain:

$$\begin{aligned}(-1)^{z_u+z_v+z_w+z_b+z_c} &= (-1)^{z_u}(-1)^{z_v}(-1)^{z_w}(-1)^{z_b}(-1)^{z_c} \\ &= m_u m_v m_w m_b m_c = m_u m_v m_w m_R m_B = -1.\end{aligned}$$

Thus, $i^{b_u+b_v+b_w} m_u m_v m_w m_E m_R^{b_u} m_B^{b_v} m_L^{b_w} = i^2 m_u m_v m_w m_R m_B = (-1)(-1) = 1.$

$\blacksquare$

Proof of Lemma 5.1: We show that each of the four operators $X_uX_vX_w$, $-X_uY_vY_wX_aX_c$, $-Y_uX_vY_wX_aX_b$, and $-Y_uY_vX_wX_bX_c$ are stabilizers of the graph state $|\phi_G\rangle$ using the properties of the Pauli gates, S gate and CZ gates. As in Example 2.1, we denote $|\psi\rangle := H^{\otimes 6}|0^6\rangle$. For clarity, we underline the set of operators rewritten or moved in each step. Note that throughout the process of rewriting, the goal is to move the X gates to the right (since they leave the state $|\psi\rangle$ fixed) and the Z gates to the left.

(i) *To show:* $X_uX_vX_w|\phi_G\rangle = |\phi_G\rangle$.

$$\begin{aligned}
&X_uX_vX_w|\phi_G\rangle = \\
&X_uX_vX_wCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = \\
&\underline{X_uCZ_{ua}}\ \underline{X_vCZ_{av}}CZ_{vb}\ \underline{X_wCZ_{bw}}CZ_{wc}CZ_{cu}|\psi\rangle = \\
&Z_aCZ_{ua}\underline{X_u}\ \underline{Z_a}CZ_{av}\ \underline{X_vCZ_{vb}}\ \underline{Z_b}CZ_{bw}\ \underline{X_wCZ_{wc}}CZ_{cu}|\psi\rangle = \\
&\underline{Z_a^2}\ Z_b\ CZ_{ua}CZ_{av}\ \underline{Z_b}\ CZ_{vb}\underline{X_v}\ CZ_{bw}\ \underline{Z_c}\ CZ_{wc}\ \underline{X_w}\ \underline{X_uCZ_{cu}}|\psi\rangle = \\
&\underline{Z_b^2}\ Z_c\ CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}\ \underline{Z_c}CZ_{cu}\underline{X_uX_wX_v|\psi\rangle} = \\
&\underline{Z_c^2}\ CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = \\
&CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = |\phi_G\rangle
\end{aligned}$$

(ii) *To show:* $-X_uY_vY_wX_aX_c|\phi_G\rangle = |\phi_G\rangle$.

$$\begin{aligned}
&-X_uY_vY_wX_aX_c|\phi_G\rangle = \\
&-\underline{X_u}Y_vY_w\underline{X_a}\ \underline{X_c}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = \\
&-Y_vY_wX_u\underline{X_aCZ_{ua}}CZ_{av}CZ_{vb}CZ_{bw}\underline{X_cCZ_{wc}}CZ_{cu}|\psi\rangle = \\
&-Y_vY_w\underline{X_uZ_u}CZ_{ua}\underline{X_aCZ_{av}}CZ_{vb}CZ_{bw}\underline{Z_w}CZ_{wc}\underline{X_cCZ_{cu}}|\psi\rangle = \\
&-Y_vY_wZ_w(-1)Z_u\underline{X_uCZ_{ua}}\ \underline{Z_v}CZ_{av}\underline{X_a}CZ_{vb}CZ_{bw}CZ_{wc}Z_uCZ_{cu}\underline{X_c|\psi\rangle} = \\
&\underline{Y_vZ_v}\ \underline{Y_wZ_w}Z_uZ_aCZ_{ua}\underline{X_u}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}Z_uCZ_{cu}\underline{X_a|\psi\rangle} = \\
&i\underline{X_v}\ i\underline{X_w}Z_uZ_aCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}\underline{X_uZ_u}CZ_{cu}|\psi\rangle = \\
&(-1)Z_uZ_aCZ_{ua}\underline{X_vCZ_{av}}CZ_{vb}\underline{X_wCZ_{bw}}CZ_{wc}(-1)\underline{Z_u}\ \underline{X_uCZ_{cu}}|\psi\rangle = \\
&\underline{Z_u^2}Z_aCZ_{ua}\underline{Z_a}CZ_{av}\underline{X_vCZ_{vb}}\ \underline{Z_b}CZ_{bw}\underline{X_wCZ_{wc}}\ \underline{Z_c}CZ_{cu}\underline{X_u|\psi\rangle} = \\
&\underline{Z_a^2}Z_bZ_cCZ_{ua}CZ_{av}\underline{Z_b}CZ_{vb}\underline{X_v}CZ_{bw}\underline{Z_c}CZ_{wc}\underline{X_w}CZ_{cu}|\psi\rangle = \\
&\underline{Z_b^2}\underline{Z_c^2}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}\underline{X_vX_w|\psi\rangle} = \\
&CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = |\phi_G\rangle
\end{aligned}$$

(iii) *To show:* $-Y_uX_vY_wX_aX_b|\phi_G\rangle = |\phi_G\rangle$.

$$-Y_uX_vY_wX_aX_b|\phi_G\rangle =$$

$$-Y_u\underline{X_v}Y_w\underline{X_a}\ \underline{X_b}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_w\underline{X_aCZ_{ua}}\ \underline{X_vCZ_{av}}\ \underline{X_bCZ_{vb}}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_wZ_uCZ_{ua}\underline{X_aZ_a}CZ_{av}\underline{X_vZ_v}CZ_{vb}\underline{X_bCZ_{bw}}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_wZ_uCZ_{ua}(-1)\underline{Z_a}\ \underline{X_aCZ_{av}}(-1)\underline{Z_v}\ \underline{X_vCZ_{vb}}\ \underline{Z_w}CZ_{bw}\underline{X_b}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_wZ_uZ_vZ_wZ_aCZ_{ua}\underline{Z_v}CZ_{av}\underline{X_a}\ \underline{Z_b}CZ_{vb}\underline{X_v}CZ_{bw}CZ_{wc}CZ_{cu}\underline{X_b|\psi\rangle} =$$

$$-Y_uY_w\underline{Z_u}\ \underline{Z_v^2}\ \underline{Z_w}Z_aZ_bCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}\underline{X_aX_v|\psi\rangle} =$$

$$-\underline{Y_uZ_u}\ \underline{Y_wZ_w}Z_aZ_bCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-i\underline{X_u}\ i\underline{X_w}Z_aZ_bCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-(-1)Z_aZ_b\underline{X_uCZ_{ua}}CZ_{av}CZ_{vb}\underline{X_wCZ_{bw}}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$Z_aZ_b\underline{Z_a}CZ_{ua}\underline{X_u}CZ_{av}CZ_{vb}\underline{Z_b}CZ_{bw}\underline{X_wCZ_{wc}}CZ_{cu}|\psi\rangle =$$

$$\underline{Z_a^2Z_b^2}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}\underline{Z_c}CZ_{wc}\underline{X_w}\ \underline{X_uCZ_{cu}}|\psi\rangle =$$

$$Z_cCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}\underline{Z_c}CZ_{cu}\underline{X_uX_w|\psi\rangle} =$$

$$\underline{Z_c^2}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = |\phi_G\rangle$$

(iv) *To show:* $-Y_uY_vX_wX_bX_c|\phi_G\rangle = |\phi_G\rangle$.

$$-Y_uY_vX_wX_bX_c|\phi_G\rangle =$$

$$-Y_uY_v\underline{X_w}\ \underline{X_b}\ \underline{X_c}\ CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_vCZ_{ua}CZ_{av}\underline{X_bCZ_{vb}}\ \underline{X_wCZ_{bw}}\ \underline{X_cCZ_{wc}}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_vCZ_{ua}CZ_{av}\underline{Z_v}CZ_{vb}X_b\underline{Z_b}\ CZ_{bw}X_w\underline{Z_w}CZ_{wc}\underline{X_cCZ_{cu}}|\psi\rangle =$$

$$-Y_uY_vZ_vZ_bZ_wCZ_{ua}CZ_{av}CZ_{vb}\underline{X_bCZ_{bw}}\ \underline{X_wCZ_{wc}}\ \underline{Z_u}CZ_{cu}\ \underline{X_c|\psi\rangle} =$$

$$-Y_uY_vZ_uZ_vZ_wZ_bCZ_{ua}CZ_{av}CZ_{vb}\underline{Z_w}\ CZ_{bw}\underline{X_b}\ \underline{Z_c}CZ_{wc}\underline{X_w}CZ_{cu}|\psi\rangle =$$

$$-Y_uY_v\underline{Z_u}\ \underline{Z_v}\ \underline{Z_w^2}Z_bZ_cCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}\underline{X_bX_w|\psi\rangle} =$$

$$-\underline{Y_uZ_u}\ \underline{Y_vZ_v}Z_bZ_cCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-(i\underline{X_u})(i\underline{X_v})Z_bZ_cCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$-(-1)Z_bZ_c\underline{X_uCZ_{ua}}\ \underline{X_vCZ_{av}}\ CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$Z_bZ_c\underline{Z_a}CZ_{ua}\underline{X_u}\ \underline{Z_a}CZ_{av}\underline{X_vCZ_{vb}}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle =$$

$$\underline{Z_a^2}Z_bZ_cCZ_{ua}CZ_{av}\underline{Z_b}CZ_{vb}\ \underline{X_v}CZ_{bw}CZ_{wc}\ \underline{X_uCZ_{cu}}|\psi\rangle =$$

$$\underline{Z_b^2}Z_cCZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}\underline{Z_c}CZ_{cu}\underline{X_uX_v|\psi\rangle} =$$

$$\underline{Z_c^2}CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}||\psi\rangle =$$

$$CZ_{ua}CZ_{av}CZ_{vb}CZ_{bw}CZ_{wc}CZ_{cu}|\psi\rangle = |\phi_G\rangle \qquad \blacksquare$$

8 Terminology

- *AC^0* - the complexity class of all polynomial-size circuits of constant-depth with unbounded fan-in gates.
- *Depth* - (of a circuit) the greatest number of gates along any (qu)bit wire of the circuit; this determines the longest path between the input and output of the circuit.
- *Entanglement* - a phenomenon in which the states of multiple qubits depend on one another.
- *Fan-in* - (of a gate) the maximum number of inputs the gate can accept; (of a circuit) the maximum fan-in of the gates in the circuit.
- *Hamming weight* - (of a bit-string) the number of non-zero bits in the string.
- *NC^0* - a subclass of AC^0, containing all polynomial-size circuits of constant-depth with bounded fan-in gates.
- *Nonlocality* - a form of correlation present in the measurement statistics of entangled quantum states that cannot be reproduced by local hidden variable models [2].
- *QNC^0* - the quantum analog of NC^0; the compelxity class of all quantum polynomial-size circuits of constant-depth with bounded fan-in gates.
- *Qubit* - Shortened form of "quantum bit", the basic unit of quantum information.
- *Shallow quantum circuits* - circuits corresponding to quantum parallel algorithms that run in constant time, take a classical bit string as input, apply a constant-depth quantum circuit composed of 1- and 2-qubit gates, and output a random bit string obtained by measuring each qubit in the standard basis [2].
- *Superposition* - a qubit's property of being able to exist in multiple states at the same time; $|\phi\rangle = c_1|\alpha\rangle + c_2|\beta\rangle$ is a superposition of the states $|\alpha\rangle$ and $|\beta\rangle$ with amplitudes $c_1, c_2 \in \mathbb{C}$.

Bibliography

[1] (2019). *Discussions with Professor Christopher King.*

[2] 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.

[3] Hoffstein, J., Pipher, J., & Silverman, J. H. (2014). *Introduction to Mathematical Cryptogrpahy.* New York City, NY: Springer-Verlag.

[4] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications.* 9(3). Retrieved from: https://arxiv.org/pdf/1804.00200.pdf.

[5] Microsoft. (2017). Pauli Measurements. Retreived from: https://docs.microsoft.com/en-us/quantum/concepts/pauli-measurements?view=qsharp-preview

[6] Nielsen, M. A. & Chuang, I. L. (2000). *Quantum Computation and Quantum Information.* New York City, NY: Cambridge University Press.

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

[8] Preskill, J. (2019). Why I Called It 'Quantum Supremacy'. *Quanta Magazine.* Retrieved from: https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy- 20191002/

[9] Shor, P. W. (1995). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Retrieved from: https://arxiv.org/pdf/quant-ph/9508027.pdf

[10] Watrous, J. (2016). Lecture 20: Bell inequalities and nonlocality. [PDF]. Retrieved from: https://cs.uwaterloo.ca/ watrous/LectureNotes/CPSC519.Winter2006/20.pdf

[11] Watts, A., Kothari, R., Schaeffer, L., & Tal, A. (2019). Exponential separation between shallow quantum circuits and unbounded fan- in shallow classical circuits. Retrieved from: https://arxiv.org/pdf/1906.08890.pdf