Black-box equivalence checking of quantum circuits by nonlocality

Weixiao Sun\textsuperscript{1,2} and Zhaohui Wei\textsuperscript{1} \textsuperscript{*}

\textsuperscript{1} Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

\textsuperscript{2} Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Suppose two quantum circuit chips are located at different places, for which we do not have any prior knowledge, and cannot see the internal structures either. If we want to find out whether they have the same functions or not with certainty, what should we do? In this paper, we show that this realistic problem can be solved from the viewpoints of quantum nonlocality. Specifically, we design an elegant protocol that examines underlying quantum nonlocality. We prove that in the protocol the strongest nonlocality can be observed if and only if two quantum circuits are equivalent to each other. We show that the protocol also works approximately, where the distance between two quantum circuits can be lower and upper bounded analytically by observed quantum nonlocality. Furthermore, we also discuss the possibility to generalize the protocol to multipartite cases, i.e., if we do equivalence checking for multiple quantum circuits, we try to solve the problem in one go. Our work introduces a nontrivial application of quantum nonlocality in quantum engineering.

I. INTRODUCTION

In the past several years, the physical realizations of quantum computing have achieved remarkable progresses \cite{1, 2}. As a result, the following three tasks have become more and more important issues in quantum computing. First, to run a quantum algorithm, which is usually designed in the language of quantum circuit, on a quantum computer, we have to compile it into a series of quantum instructions that can be executed directly on the quantum hardware, and as a whole this is essentially another quantum circuit. Second, when executing quantum instructions on a quantum computer, the hardware configuration has to be respected, which means that the available quantum instructions are actually restricted. If this is not the case, we have to map the quantum circuit at hand into another desirable one. Third, for now the scaling of quantum computing is still small, and quantum computational resources are very precious, therefore it is always nice to make sure that the executed quantum circuit has been optimized.

It is not hard to see that a common part in the above three issues is that sometimes we need to transfer a quantum circuit into another. Undoubtedly, during these transformations a fundamental requirement is that the initial quantum circuit and the output have to be functionally equivalent exactly. As a consequence, equivalent checking of quantum circuits is a profound problem in quantum computing and quantum engineering.

In fact, this problem has attracted a lot of attentions, and quite a few approaches have been proposed accordingly. Particularly, in \cite{3} an approach based on decision diagrams was proposed for equivalence checking of quantum circuits, where the central idea is representing quantum circuits as decision programs, on which the comparisons are performed. In \cite{4}, a concept called reversible miter was proposed for this problem, which is a generalization of miter circuits utilized in digital electronic circuits, and can be integrated with circuit simplifications and decision programs techniques. Meanwhile, as mentioned above, equivalence checking of quantum circuits have been extensively studied in the optimization of quantum circuits and the verifications of quantum compilers \cite{5–10}. Very recently, equivalence checking has also been introduced to handle sequential quantum circuits, where a Mealy machine-based framework was proposed \cite{11}.

Despite these encouraging approaches for equivalence checking of quantum circuits, however, they share the common feature that internal structures of involved quantum circuits can be seen. If we use the language of software testing, this is essentially a kind of white-box testing. Then like in software testing, black-box testing should be another scenario that needs to be considered for equivalence checking of quantum circuits.

Indeed, suppose we have two manufactured quantum circuit chips that are separated and the insides cannot be seen, then it is still a realistic and important problem for us to find out whether they have the same functions with certainty. Trying to solve this problem is the main target of the current paper. We stress that in our setting we do not have any prior knowledge on quantum circuits to be compared, and this is essentially different from the topic of unitary operation discrimination \cite{12, 14}, where every unitary operation is picked up from a small set known beforehand.

In this paper, based on the key role played by quantum nonlocality, we design an elegant approach that can achieve black-box equivalence checking of quantum circuits with certainty. Clearly, no similar approach exists for the classical counterpart of this problem. Particularly, we provide a complete mathematical characterization for our approach. First, we prove that in our protocol, the observed quantum nonlocality is the strongest if and only if the two involved quantum circuits have exactly the same functions. Second, we show that the

\textsuperscript{*} Email: weizhaohui@gmail.com
protocol also works well in the approximate sense, i.e., for a given strength of observed quantum nonlocality, we provide analytical lower and upper bounds for the distance between the two quantum circuits. By providing numerical evidences, we show that the above bounds have very good performance. Lastly, we discuss the possibility to generalize our protocol to the case of multiple quantum circuits, where we want to determine whether three or more quantum circuits are equivalent to each other in one go. We argue that at least when the number of quantum circuits is odd, this is impossible. Our results provide a new way to apply quantum nonlocality to solve important problems in future quantum engineering.

II. THE EQUIVALENCE CHECKING OF TWO QUANTUM CIRCUITS

A. The exact case

Suppose two $n$-qubit quantum circuits $C_1$ and $C_2$ are held by two separated players, Alice and Bob, respectively. Since Hadamard gate and Toffoli gate form a universal gate set for quantum computation [15], without loss of generality we suppose that the matrix representations of $C_1$ and $C_2$ are real, denoted $U_1$ and $U_2$. Then our task is to determine whether $U_1$ is equivalent to $U_2$ up to a global phase (since they are real, a global phase can only be $\pm 1$). Let us first consider the smallest case where $C_1$ and $C_2$ are single-qubit quantum circuits.

Before introducing our main idea, let us recall some facts on quantum nonlocality and Bell experiments. Suppose Alice and Bob share a lot of EPR pairs, i.e.,

$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

On each EPR pair, they repeat the following procedure. Both of them perform random local measurements on their qubits respectively, where Alice measures observables

$$A_0 = \sigma_X, \quad A_1 = \sigma_Z,$$

and Bob measures observables

$$B_0 = (\sigma_X + \sigma_Z)/\sqrt{2}, \quad B_1 = (\sigma_X - \sigma_Z)/\sqrt{2}.$$  \hspace{1cm} (3)

Here $\sigma_X$ and $\sigma_Z$ are Pauli matrices. Then they calculate all the probability distribution $p(ab|xy)$, i.e., the probability that Alice and Bob obtain outcomes $a$ on $A_x$ and $b$ on $B_y$, respectively, where $a, b \in \{-1, 1\}$ and $x, y \in \{0, 1\}$. Let $\langle A_x B_y \rangle = \sum_{a,b} ab p(ab|xy)$, and

$$I_{\text{CHSH}} = \langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_1 B_1 \rangle,$$  \hspace{1cm} (4)

then it holds that $I_{\text{CHSH}} = 2\sqrt{2}$. As a comparison, if $p(ab|xy)$ is produced by a classical system, the corresponding value will not be larger than 2, and this is the famous Clauser-Horne-Shimony-Holt (CHSH) inequality [16]. A well-known fact is that the above violation to the CHSH inequality achieved by EPR pairs is optimal [16], which is the foundation of many quantum information processing tasks [17–19].

We now change the above Bell experiment a little bit by adding one more step. Before measuring each EPR pair, Alice and Bob input the qubit they hold into $C_1$ and $C_2$ respectively, then the overall output will be

$$|\psi\rangle = \frac{1}{\sqrt{2}}(U_1 |0\rangle \otimes U_2 |0\rangle + U_1 |1\rangle \otimes U_2 |1\rangle),$$  \hspace{1cm} (5)

on which they perform the same sets of local measurements as above. Here we stress that it is crucial to use the same sets of local measurements. We now analyze the new value of $I'_{\text{CHSH}}$, denoted $I'_{\text{CHSH}}$.

We first consider the case that $U_1 = U_2$. Recall that they are real unitary matrices, then by a straightforward calculation it can be verified that $|\psi\rangle = |\text{EPR}\rangle$, which means $I'_{\text{CHSH}} = 2\sqrt{2}$. That is to say, if $C_1$ and $C_2$ are the same, the above experiment will still result in the maximal violation to the classical bound. In this situation, it is natural to ask, is the converse correct? That is, does $I'_{\text{CHSH}} = 2\sqrt{2}$ always imply that $U_1 = U_2$? If this is correct, then we can perfectly determine whether $C_1$ and $C_2$ are equivalent by performing the above modified Bell experiment.

Actually, this is indeed the case. Indeed, it has been known that if $I'_{\text{CHSH}} = 2\sqrt{2}$, the following conditions are satisfied [17].

$$\frac{A_0 + A_1}{\sqrt{2}} |\psi\rangle = B_0/B_1 |\psi\rangle.$$  \hspace{1cm} (6)

By straightforward calculations, it can be verified that this indicates that $|\psi\rangle = |\text{EPR}\rangle$ up to a global phase. On the other hand, if $U_1 \neq \pm U_2$, it can be checked that $|\psi\rangle \neq \pm |\text{EPR}\rangle$, which means that if $I'_{\text{CHSH}} = 2\sqrt{2}$, we must have $U_1 = U_2$.

We now move to the general case, where the common size of $C_1$ and $C_2$ is $n$ qubits, and $n > 1$ is an arbitrary integer. Let $d = 2^n$. Inspired by the single-qubit case, Alice and Bob hope they can use a similar protocol to find out whether $C_1$ and $C_2$ are equivalent. That is to say, they hope that the following plan could be realized. Again, they first prepare and share many copies of the maximally entangled state

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle,$$  \hspace{1cm} (7)

and choose a certain Bell inequality such that $|\Phi_d\rangle$ violates it maximally, where they record the local measurements that achieve the maximal violation. Then similarly, for each copy of $|\Phi_d\rangle$, Alice and Bob input their own subsystems into the corresponding quantum circuits they hold respectively. On the output state, which is
now \((U_1 \otimes U_2)|\Phi_d\rangle\), they perform the same local measurements as recorded above. By repeating the experiments, they collect the measurement outcome statistics data \(p(ab|xy)\), where \(x, y \in \{1, 2, \ldots, m\}\) and \(a, b \in \{0, 1, \ldots, d - 1\}\) are the labels for the local measurements and the corresponding outcomes. Then they examine the measurement outcome statistics data with the above chosen Bell inequality, and hope that \((U_1 \otimes U_2)|\Phi_d\rangle\) violates the Bell inequality maximally if and only if \(U_1 = U_2\) up to a global phase.

Clearly, if the above Bell equality exists, like in the qubit case, Alice and Bob can determine whether \(C_1\) and \(C_2\) are equivalent perfectly according to the violation. Again, a key question is, can we find such a Bell inequality when \(n > 1\)? It turns out that, once more, the answer is positive.

According to our plan, such a desirable Bell inequality should be violated maximally by maximally entangled states. However, it has been well-known that entanglement is a different resource from quantum nonlocality, and on many Bell inequalities it is not maximally entangled states that achieve the maximal violations, say the Collins-Gisin-Linden-Masser-Popescu (CGLMP) inequalities [20]. In the meantime, quantum nonlocality can be observed directly by quantum experiments, while entanglement cannot, thus we often choose to characterize unknown entanglement by looking into the underlying quantum nonlocality. Therefore, when doing this, we hope that quantum nonlocality we observed and the underlying entanglement are as consistent as possible, which implies that the above desirable Bell inequalities will be nice choices. Interestingly, in [21] such a class of beautiful Bell inequalities have been proposed, which were deliberately designed to be violated maximally by \(|\Phi_d\rangle\).

Specifically, to perform the measurement labelled by \(x\), Alice measures an observable with eigenvectors \(|a\rangle_x\) \((a = 0, 1, \ldots, d - 1, \) and \(x = 1, 2, \ldots, m)\), and

\[|a\rangle_x = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp \left[ \frac{2\pi i}{d} k(a - \alpha_x) \right] |k\rangle, \tag{8} \]

where \(i = \sqrt{-1}\) is the imaginary number, and \(\alpha_x = (x - 1/2)/m\). Similarly, to perform the measurement labelled by \(y\), Bob measures an observable with eigenvectors \(|b\rangle_y\) \((b = 0, 1, \ldots, d - 1, \) and \(y = 1, 2, \ldots, m)\), and

\[|b\rangle_y = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp \left[ -\frac{2\pi i}{d} k(b - \beta_y) \right] |k\rangle, \tag{9} \]

where \(\beta_y = y/m\). On an arbitrary quantum state \(|\phi\rangle\), the Bell expression is essentially equivalent to

\[I_{d,m}(|\phi\rangle) = \sum_{i=1}^{m} \sum_{l=1}^{d-1} \langle\Phi| (A_i^l \otimes B_i^l) |\phi\rangle, \tag{10} \]

where \(A_i = \sum_{a=0}^{d-1} \omega^{a \alpha_i} |a\rangle_i |i\rangle\), \(B_i = (A_i)^*\), and \(\omega = \exp(2\pi i/d)\). Note that \(A_i^l\) and \(B_i^l\) are unitary matrices.

In [21], it was proved that the Tsirelson bound of \(I_{d,m}\) is \(m(d-1)\), which is achieved exactly by \(|\Phi_d\rangle\) and strictly larger than the classical bound. Indeed, a property of \(|\Phi_d\rangle\) is that for any \(d \times d\) matrices \(M\) and \(N\), it holds that

\[(M \otimes N)|\Phi_d\rangle = (I \otimes NM^T)|\Phi_d\rangle. \tag{11} \]

Since \(B_i^l = (A_i^l)^*\) for any \(i\) and \(l\), we have that

\[\langle\Phi| (A_i^l \otimes B_i^l)|\Phi\rangle = \langle\Phi| (I \otimes \Phi)|\Phi\rangle = 1, \tag{12} \]

implying that \(I_{d,m} = m(d-1)\) on this state.

Let us go back to our task. We first notice that if \(C_1\) and \(C_2\) are the same, i.e., \(U_1 = U_2 = U\), \((U_1 \otimes U_2)|\Phi_d\rangle\) always achieves the Tsirelson bound of \(I_{d,m}\). In fact, for any \(i\) and \(l\) it holds that

\[\langle\Phi| (U^T \otimes U^T)(A_i^l \otimes B_i^l)(U \otimes U)|\Phi\rangle = \langle\Phi| (I \otimes U^T B_i^l U U^T A_i^l)^T U|\Phi\rangle = \langle\Phi| (I \otimes I)|\Phi\rangle \]

Implies that \(I_{d,m} = m(d-1)\) in this situation, similar to the case of single-qubit quantum circuits, we need to consider whether the converse is correct or not. Or, can we have \(U_1 \neq U_2\) but \(I_{d,m}(|U_1 \otimes U_2|\Phi_d\rangle) = m(d-1)\)? We now show that this is impossible.

**Theorem 1** \(I_{d,m}(|U_1 \otimes U_2|\Phi_d\rangle) = m(d-1)\) if and only if \(U_1 = U_2\) up to a global phase.

**Proof** We only need to prove that \(I_{d,m}(|U_1 \otimes U_2|\Phi_d\rangle) = m(d-1)\) implies \(U_1 = U_2\). According to the definition of \(I_{d,m}\), we know that if \(I_{d,m}(|U_1 \otimes U_2|\Phi_d\rangle) = m(d-1)\), each term in the summation of Eq. (10) will be 1. Therefore, for any \(i \in \{1, 2, \ldots, m\}\), it holds that (let \(l = 1\))

\[\langle\Phi| (U_1^T \otimes U_2^T)(A_i^l \otimes B_i^l)(U_1 \otimes U_2)|\Phi\rangle = \langle\Phi| (I \otimes U_2^T B_i^l U_2 U_1^T A_i^l)^T U_1|\Phi\rangle = \frac{1}{d} \text{Tr}(U_2^T B_i^l U_2 U_1^T A_i^l)^T U_1 \]

\[= \frac{1}{d} \text{Tr}(U_1 U_2^T B_i^l U_1^T A_i^l)^T U_1 \]

\[= 1, \]

where we have utilized the fact that for any \(d \times d\) matrices \(M\) and \(N\), it holds that \(\langle\Phi| (I \otimes M)|\Phi\rangle = \text{Tr}(MN)/d\) and \(\text{Tr}(MN) = \text{Tr}(NM)\). Hence, we obtain that \(\text{Tr}(U_1 U_2^T B_i^l U_2 U_1^T A_i^l)^T = d\).

Meanwhile, note that \(U_1 U_2^T B_i^l U_2 U_1^T (A_i^l)^T = I\). For simplicity, let \(S_1 = U_2 U_1^T\) and \(S_2 = B_i^l\). Then this means \(S_1^T S_2 S_1 = I\), which is also \(S_2 S_1 = S_1 S_2\), where we have utilized the fact that both \(S_1\) and \(S_2\) are unitary matrices. Since \(S_1\) and \(S_2\) are also normal matrices, this shows that they can be simultaneously diagonalizable.
Similarly, let \( j \neq i \in \{1, 2, ..., m\} \) and \( S_3 = \overline{B}_1^1 \), then \( S_1 \) and \( S_3 \) can also be simultaneously diagonalizable. Recall the definition of \( B_1^1 \), whose eigenvectors are given by the conjugate of Eq.\([8]\), then we have that \( S_1 \) can be diagonalized in the following two different ways,

\[
S_1 = \sum_{a=0}^{d-1} g_a(a) |a\rangle \langle a| = \sum_{a=0}^{d-1} h_a(a) |a\rangle \langle a| \quad ,
\]

where for any \( a \), \( g_a \) and \( h_a \) are unit complex number. Then

\[
g_0 = h_0 = ... = h_{d-1} = e^{i\gamma},
\]

which implies that \( S_1 = e^{i\gamma} \cdot I \). According to the definition of \( S_1 \), we now have that \( U_1 = U_2 \) up to a global phase, which completes the proof.

The theorem shows the correctness of our plan, and we can indeed determine whether \( U_1 \) and \( U_2 \) have the same function by examining the underlying quantum nonlocality of \( (U_1 \otimes U_2) |\Phi_d\)\).

B. The approximate case

Since equivalent checking is an important issue in engineering applications, we need to address the situation that quantum circuits are realized approximately. That is, if the above Bell expression value \( I_{d,m}((U_1 \otimes U_2) |\Phi_d)\) is not exactly \( m(d-1) \), can we draw any nontrivial conclusions on \( D(U_1, U_2) \), the distance between \( U_1 \) and \( U_2 \)? We now show that this is indeed the case, and furthermore, for a given value of \( I_{d,m}((U_1 \otimes U_2) |\Phi_d)\), \( D(U_1, U_2) \) can be lower and upper bounded analytically.

In this paper, we choose the definition for \( D(U_1, U_2) \) as the one given by [23], which is

\[
D(U_1, U_2) = \sqrt{1 - \frac{1}{d} \text{Tr}(U_1^2 U_2^2)}.
\]

Meanwhile, we need to use the following key fact, whose proof can be seen in the Appendix.

Lemma 1 Suppose \( |\psi\rangle \) is a \( d \times d \) quantum state orthogonal to \( |\Phi_d\rangle \). Then

\[
-m \leq I_{d,m}(|\psi\rangle) \leq m(d-2).
\]

Having this fact, we are ready to give the second main result of the current paper.

Theorem 2 Suppose \( V = I_{d,m}((U_1 \otimes U_2) |\Phi_d)\), then we have that

\[
\sqrt{1 - \frac{V + m}{md}} \leq D(U_1, U_2) \leq \sqrt{1 - \frac{V - m(d-2)}{m}}.
\]

Proof Let \( |\alpha\rangle = (U_1 \otimes U_2) |\Phi_d) = (I \otimes U_2 U_1^T) |\Phi_d\)\). Suppose an orthogonal decomposition of \( U_2 U_1^T \) is \( U_2 U_1^T = \sum_{j=0}^{d-1} e^{i\theta_j} |\lambda_j\rangle \langle \lambda_j| \), where \( \theta_j \in [0, 2\pi] \). Note that we also have

\[
|\Phi_d) = \sum_{j=0}^{d-1} |\lambda_j\rangle \langle \lambda_j| / \sqrt{d}.
\]

Therefore, we have that

\[
|\alpha\rangle = \sum_{j=0}^{d-1} e^{i\theta_j} |\lambda_j\rangle \langle \lambda_j| / \sqrt{d}.
\]

Let \( |\alpha\rangle = c_1 |\Phi_d) + c_2 |\Phi^\perp) \), where \( c_1 \) and \( c_2 \) are complex numbers, \( |c_1|^2 + |c_2|^2 = 1 \), and \( |\Phi^\perp) |\Phi_d) = 0 \). Then it can be seen that

\[
c_1 = \langle \Phi_d |\alpha\rangle = \sum_{j=0}^{d-1} e^{i\theta_j} \frac{\text{Tr}(U_2 U_1^T)}{d},
\]

which means that \( D(U_1, U_2)^2 = 1 - |c_1|^2 \).

For convenience, let \( B = \sum_{i=1}^{m} \sum_{d=1}^{d-1} (A^i_d \otimes \overline{B}_1^1) \). Then it holds that

\[
V = \langle \alpha | B |\alpha\rangle = (c_1^* \langle \Phi_d | + c_2^* \langle \Phi^\perp |)B(c_1 |\Phi_d) + c_2 |\Phi^\perp) \rangle
= |c_1|^2 \langle \Phi_d | B |\Phi_d) + c_2^2 \langle \Phi^\perp | B |\Phi^\perp) \rangle
= |c_1|^2 \cdot m(d-1) + (1 - |c_1|^2) \langle \Phi^\perp | B |\Phi^\perp) \rangle.
\]

According to Lemma 1, we have that \( -m \leq \langle \Phi^\perp | B |\Phi^\perp) \rangle \leq m(d-2) \), which means that

\[
\sqrt{V - m(d-2)} \leq |c_1| \leq \sqrt{V + m}.
\]

Combining this with the fact that \( D(U_1, U_2)^2 = 1 - |c_1|^2 \), we complete the proof.

Note that when \( V = m(d-1) \), both the lower and the upper bounds are exactly 1, implying that both of them are tight in this case. When \( V \) does not achieve \( m(d-1) \), the lower bound for \( D(U_1, U_2) \) reveals the minimum distance between \( U_1 \) and \( U_2 \), thus in some sense it is more informative than the upper bound.

It should also be pointed out that to examine quantum nonlocality, we need to collect all the data of form \( p(ab|xyz) \), which have \( m^2 d^2 \) terms. If we choose \( m = 2 \), then this number becomes \( 4d^2 \). In other words, in our protocol the number of measurements we have to perform is a polynomial of \( d \).

To examine the performance of the above analytical bounds further, we test them with numerical calculations. For this, we generate many random instances for \( U_1 \) and \( U_2 \), then we compute the corresponding values of \( D(U_1, U_2) \) and \( V \) to make the comparisons. The results are listed in Fig.4, where it can be seen that the lower bound is quite tight in many instances.
satisfy that condition that for any local unitary matrix
quantum state $|\psi_k\rangle$ we have that $k$ is even, where the major challenge is to find a desirable multipartite Bell inequality. We leave this for future work.

IV. DISCUSSIONS

In this paper, we have proposed a protocol for blackbox equivalence checking of quantum circuits, where the key quantum property we have utilized is quantum nonlocality. We have proved the correctness of our protocol analytically and numerically. Particularly, for real life applications we have showed that for any given strength of observed quantum nonlocality, the distance between two quantum circuits can be lower and upper bounded analytically. Our work can be regarded as a nontrivial application of quantum nonlocality in the area of quantum engineering. Considering the rise of this area in recent years and the fundamentality of the problem our protocol addresses, we hope this protocol can be applied in future quantum industries.

ACKNOWLEDGMENTS

This work was supported by the National Key R&D Program of China, Grant No. 2018YFA0306703, and the National Natural Science Foundation of China, Grant No. 20181311604. This work was also supported in part by the Zhongguancun Haihua Institute for Frontier Information Technology.

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al., Nature 574, 505 (2019).
[2] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, et al., Science 370, 1460 (2020).
[3] G. F. Viamontes, I. L. Markov, and J. P. Hayes, in 2007 IEEE/ACM International Conference on Computer-Aided Design (IEEE, 2007) pp. 69–74.
[4] S. Yamashita and I. L. Markov, in 2010 IEEE/ACM International Symposium on Nanoscale Architectures (IEEE, 2010) pp. 23–28.
[5] M. Amy, D. Maslov, and M. Mosca, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33, 1476 (2014).
[6] Y. Nam, N. J. Ross, Y. Su, A. M. Childs, and D. Maslov, npj Quantum Information 4, 1 (2018).
[7] A. Kissinger and J. van de Wetering, arXiv preprint arXiv:1903.10477 (2019).
[8] K. N. Smith and M. A. Thornton, in Proceedings of the 46th International Symposium on Computer Architecture (2019) pp. 579–588.
arXiv:1908.08963 (2019).
[10] K. Hietala, R. Rand, S.-H. Hung, X. Wu, and M. Hicks, Proceedings of the ACM on Programming Languages 5, 1 (2021).
[11] Q. Wang and M. Ying, arXiv preprint arXiv:1811.07722 (2018).
[12] A. Acin, Physical Review Letters 87, 177901 (2001).
[13] G. M. D’Ariano, P. L. Presti, and M. G. Paris, Physical Review Letters 87, 270404 (2001).
[14] R. Duan, Y. Feng, and M. Ying, Physical Review Letters 98, 100503 (2007).
[15] Y. Shi, Quantum Information & Computation 3, 84 (2003).
[16] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Physical Review Letters 23, 880 (1969).
[17] S. Popescu, Physical Review Letters 88, 040404 (2002).
[18] D. Mayers and A. Yao, in Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280) (IEEE, 1998) pp. 503–509.
[19] A. K. Ekert, Physical Review Letters 67, 661 (1991).
[20] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Physical Review Letters 88, 040404 (2002).
[21] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Physical Review Letters 119, 040402 (2017).
[22] A. Montanaro and R. de Wolf, Theory of Computing, 1 (2016).

V. APPENDIX

Lemma 2 Suppose $|\psi\rangle$ is a $d \times d$ quantum state orthogonal to $|\Phi_d\rangle$. Then

\[ -m \leq I_{d,m}(|\psi\rangle) \leq m(d-2). \]  \hspace{1cm} (22)

Proof Recall that $A_x^1 = \sum_{a=0}^{d-1} \omega^a |a\rangle_x \langle a|$, and $B_x^1 = A_x^1$, where

$|a\rangle_x = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left[ \frac{2\pi i}{d} k(a - \alpha_x) \right] |k\rangle.$

Then it holds that

$A_x^1 \otimes B_x^1 = \sum_{a,b=0}^{d-1} \omega^{a-b} |a\rangle_x \langle a| \otimes |(b\rangle_x \langle b)|^*,$

and

$|b\rangle_x^* = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \exp\left[ -\frac{2\pi i}{d} k(b - \alpha_x) \right] |k\rangle.$

For a fixed $x$, let $|\psi\rangle = \sum_{a,b=0}^{d-1} \beta_{ab,x}|a\rangle_x |b\rangle_x^*$. Then we have that

$\langle \psi | A_x^1 \otimes B_x^1 |\psi\rangle = \sum_{a=0}^{d-1} \sum_{b=0}^{d-1} |\beta_{ab,x}|^2 \omega^{a-b},$

and

$\sum_{l=1}^{d-1} \langle \psi | A_x^l \otimes B_x^l |\psi\rangle = \sum_{l=1}^{d-1} \sum_{a=0}^{d-1} \sum_{b=0}^{d-1} |\beta_{ab,x}|^2 \omega^{l(a-b)}$

\[ = \sum_{a=0}^{d-1} |\beta_{aa,x}|^2 (d-1) + \sum_{a \neq b} |\beta_{ab,x}|^2 (-1) \]

\[ = d \sum_{a=0}^{d-1} |\beta_{aa,x}|^2 - 1, \]

which implies that

$\sum_{x=1}^{m} \sum_{l=1}^{d-1} \langle \psi | A_x^l \otimes B_x^l |\psi\rangle = \sum_{x=1}^{m} \sum_{a=0}^{d-1} |\beta_{aa,x}|^2 - m.$

Then it is not hard to see that

$I_{d,m}(|\psi\rangle) \geq -m.$

At the same time, we let $|\psi\rangle = \sum_{j=0}^{d-1} \sum_{a=0}^{d-1} \gamma_{kj} |j\rangle$. As it is orthogonal to $|\Phi_d\rangle$, we obtain that

$\sum_{k=0}^{d-1} \gamma_{kk} = 0.$

Note that

$|a\rangle_x |a\rangle_x^* = \frac{1}{d} \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} \exp\left[ \frac{2\pi i}{d} (k-j)(a - \alpha_x) \right] |k\rangle |j\rangle,$

thus we have

$\beta_{aa,x} = \frac{1}{d} \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} \exp\left[ \frac{2\pi i}{d} (j-k)(a - \alpha_x) \right] \gamma_{kj}.$

As a result,
\[
\sum_{x=1}^{m} \sum_{l=1}^{d-1} (\psi|A^*_x \otimes B^*_l|\psi) = d \sum_{x=1}^{m} \sum_{a=0}^{d-1} |\beta_{a,x}|^2 - m
\]

\[
= \frac{1}{d} \sum_{x=1}^{m} \sum_{a=0}^{d-1} \left( \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} \exp \left[ \frac{2\pi i}{d}(j-k)(a-\alpha_x) \right] \gamma_{kj} \right)^2 - m
\]

\[
= \frac{1}{d} \sum_{x=1}^{m} \sum_{a=0}^{d-1} \left( \sum_{k=0}^{d-1} \sum_{r=0}^{d-1} \exp \left[ \frac{2\pi i}{d} r(a-\alpha_x) \right] \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \exp \left[ \frac{2\pi i}{d} (r-d)(a-\alpha_x) \right] \gamma_{k(k+r-d)} \right)^2 - m
\]

\[
= \frac{1}{d} \sum_{x=1}^{m} \sum_{a=0}^{d-1} \left( \sum_{k=0}^{d-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \gamma_{k(k+r-d)} \right)^2 - m
\]

where we have defined the matrix \(V_x\) and the vector \(\vec{z}_x\) by setting their entries to be

\[
(V_x)_{a,r} = \frac{\exp \left[ \frac{2\pi i}{d} r(a-\alpha_x) \right]}{\sqrt{d}}.
\]

\[
(\vec{z}_x)_k = \sum_{k=0}^{d-r-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \exp \left[ 2\pi i \alpha_x \right] \gamma_{k(k+r-d)}.
\]

It can be verified that \(V_x\) is unitary, then we have \(|V_x \vec{z}_x| = |\vec{z}_x|\). So

\[
\sum_{x=1}^{m} |V_x \vec{z}_x|^2 - m
\]

\[
= \sum_{x=1}^{m} |\vec{z}_x|^2 - m
\]

\[
= \sum_{x=1}^{m} \sum_{a=0}^{d-1} \sum_{r=0}^{d-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \exp \left[ 2\pi i \alpha_x \right] \gamma_{k(k+r-d)} \right)^2 - m
\]

It can be verified that \(\forall a, b, \lambda_k \in \mathbb{C}, \text{ if } \sum_{k=0}^{m} \lambda_k = 0 \text{ and } |\lambda_k| = 1, \text{ we have } \sum_{k=1}^{m} |a + \lambda_k b|^2 = m(|a|^2 + |b|^2). \text{ Then it holds that}

\[
\sum_{x=1}^{m} \sum_{a=0}^{d-1} \sum_{r=0}^{d-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \exp \left[ 2\pi i \alpha_x \right] \gamma_{k(k+r-d)} \right)^2 - m
\]

\[
= m \sum_{x=1}^{m} \sum_{r=0}^{d-1} \left( \sum_{k=0}^{d-r-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \gamma_{k(k+r-d)} \right)^2 - m
\]

\[
= m \sum_{r=1}^{d-1} \left( \sum_{k=0}^{d-r-1} \gamma_{k(k+r)} + \sum_{k=d-r}^{d-1} \gamma_{k(k+r-d)} \right)^2 - m
\]

\[
\leq m \sum_{r=1}^{d-1} \left( (d-r) \sum_{k=0}^{d-r-1} |\gamma_{k(k+r)}|^2 + r \sum_{k=d-r}^{d-1} |\gamma_{k(k+r-d)}|^2 \right) - m
\]

\[
\leq m(d-1) \sum_{r=1}^{d-1} \left( \sum_{k=0}^{d-r-1} |\gamma_{k(k+r)}|^2 + \sum_{k=d-r}^{d-1} |\gamma_{k(k+r-d)}|^2 \right) - m
\]

\[
\leq m(d-2).
\]