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. In such a situation, a realistic and fundamental problem is to find out whether they have the same functions or not with certainty. In this paper, we show that this problem can be solved completely from the viewpoint of quantum nonlocality. Specifically, we design an elegant protocol that examines underlying quantum nonlocality, where 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 calculated accurately by observing quantum nonlocality in an analytical manner. Furthermore, it turns out that the computational cost of our protocol is independent of the size of compared quantum circuits. Lastly, 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.

In the past several years, physical realizations of quantum computing have achieved remarkable progresses. As a result, the following four tasks are becoming more and more important in quantum computing. First, to run a quantum algorithm, which is usually designed in the language of a 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. Fourth, quantum computing has been physically implemented on different quantum platforms, then if we run the same quantum algorithm on different platforms, an important problem is to make sure they are essentially the same, where the quantum circuits may look different.

It is not hard to see that a common part of the above four fundamental problems is that we need to transfer a quantum circuit into another or compare two quantum circuits. Undoubtedly, during these transformations or comparisons, a basic requirement is to find out whether an initial quantum circuit and the compiled, optimized, or compared quantum circuit have exactly the same functions. As a consequence, equivalent checking of quantum circuits is a profound problem in quantum computing and quantum engineering. We stress that sometimes the compared two quantum circuits are located at different places.

In fact, this problem has attracted a lot of attention, and quite a few approaches have been proposed accordingly. Particularly, in ref. 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 ref. , 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 program techniques. Meanwhile, as mentioned above, equivalence checking of quantum circuits has been extensively studied in the optimization of quantum circuits and the verification of quantum compilers. Very recently, equivalence checking has also been introduced to handle sequential quantum circuits, where a Mealy machine-based framework was proposed.

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 that the internal structures of quantum circuits cannot be seen and should also be a realistic scenario that needs to be considered.

Indeed, as mentioned, in the future it will be an important problem for us to find out whether two separated manufactured quantum circuit chips that the insides cannot be seen 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 of quantum circuits to be compared, and this is essentially different from the topic of unitary operation discrimination, 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 protocol also works well in an 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 evidence, we verify the
correctness of these bounds. Third, by looking into the
structure of the gap between the above two bounds, we
proposed a modified protocol such that the gap disappears,
which means that based on the observed nonlocality we can
completely pin down the distance between the compared
quantum circuits generally. Fourth, we analyze the computa-
tional cost of the modified protocol and show that it is
independent of the size of compared quantum circuits. That is,
for a given precision we need only a constant cost to check the
equivalence of large quantum circuits. Lastly, we discuss the
possibility to generalize our protocol to the case of multiple
quantum circuits, where we want to determine whether three
or even 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. We believe that our results
demonstrate a possibility to apply quantum nonlocality to
important problems in future quantum engineering.

RESULTS
The exact equivalence checking of two quantum circuits
Suppose two d-dimensional quantum circuits $C_1$ and $C_2$ are
held by two separated players, Alice and Bob, respectively. Since
the Hadamard gate and the Toffoli gate form a universal gate set
for quantum computation\textsuperscript{15}, and the matrix
representations for both of the two quantum gates involve only real
numbers, quantum circuits with real matrix representations already enjoy
the full power of quantum computation. Because of this fact, in this work,
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., $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. On
each EPR pair, they repeat the following procedure. Both of
them perform random local measurements on their qubits
respectively, where Alice measures observables $A_0 = \sigma_x$ and
$A_1 = \sigma_z$, and Bob measures observables $B_0 = (\sigma_x + \sigma_z)/\sqrt{2}$ and
$B_1 = (\sigma_x - \sigma_z)/\sqrt{2}$. Here $\sigma_x$ and $\sigma_z$ are Pauli matrices. Then they
calculate all the probability distribution $p(ab|x,y)$, i.e., the
probability that Alice and Bob obtain outcomes $a$ on $A_0$ and $b$ on
$B_y$ respectively, where $a, b \in \{-1, 1\}$ and $x, y \in \{0, 1\}$. Let
$\langle A_iB_j \rangle = \sum_{a,b} p(ab|x,y)$, and

$$I_{\text{CHSH}} = (A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1),$$

then it holds that $|I_{\text{CHSH}}| < 2\sqrt{2}$. As a comparison, if $p(ab|x,y)$ is
produced by a classical system, the corresponding value will not be
larger than $2$, and this is the famous Clauser–Home–Shimony–Holt
(CHSH) inequality\textsuperscript{16}. A well-known fact is that the above violation of
the CHSH inequality achieved by EPR pairs is optimal\textsuperscript{15}, which is the
foundation of many quantum information processing tasks\textsuperscript{15,16}.

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 $|\psi\rangle = \frac{1}{\sqrt{2}}(U_1|0\rangle \otimes U_2|0\rangle + U_1|1\rangle \otimes U_2|1\rangle)$, 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 $I_{\text{CHSH}}^d$.

We first consider the case that $U_1 = U_2$. Recall that they are real
unitary matrices, then it can be verified that $|\psi\rangle = |EPR\rangle$, which
means $I_{\text{CHSH}}^d = 2\sqrt{2}$. That is to say, if $C_1$ and $C_2$ are the same, the
above experiment will still result in a maximal violation. In this
situation, a natural problem is to find out whether the converse is
correct or not, i.e., whether or not $I_{\text{CHSH}}^d = 2\sqrt{2}$ always implies
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. It has been known that if

$$I_{\text{CHSH}}^d = 2\sqrt{2},$$

the following conditions are satisfied\textsuperscript{17}.

$$A_0 \pm A_1 = \frac{1}{\sqrt{2}} |B_0/1\rangle \langle \psi|.$$  

By straightforward calculations, it can be verified that this
indicates that $|\psi\rangle = |EPR\rangle$ up to a global phase. On the other hand, if $U_1 \neq \pm U_2$, it can be checked that $|\psi\rangle \neq \pm |EPR\rangle$, which
means that if $I_{\text{CHSH}}^d = 2\sqrt{2}$, 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 $d$-dimensional. 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, they hope that the
following plan could be realized. Again, they first prepare and
share many copies of the maximally entangled state

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle.$$  

Note that if the quantum circuits are based on qubits, $|\Phi_d\rangle$ can be
prepared by combining $n$ EPR pairs together. Then they choose
a certain Bell inequality such that $|\Phi_d\rangle$ violates it maximally, while
they record the local measurements that achieve the maximal
violation. Then 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 $p(ab|x,y)$, where $x, y \in \{1, 2, ..., m\}$ and $a, b \in \{0, 1, \ldots, d-1\}$ are the labels for the local
measurements and the corresponding outcomes. Then they examine the above 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. Interestingly, it turns out that
such a Bell inequality does exist.

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–Masner–Popescu (CGLMP) inequal-
ities\textsuperscript{18}. 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 the quantum nonlocality we observed
and the underlying entanglement is as consistent as possible,
which implies that the above desirable Bell inequalities will be
nice choices. Fortunately, in ref.\textsuperscript{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 labeled by $x$, Alice
measures an observable with eigenvectors $|a\rangle_x$ ($a = 0, 1, \ldots, d-1$, and $x = 1, 2, \ldots, m$), and

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

where $i = \sqrt{-1}$ is the imaginary number, and $a_x = (x-1/2)/m$.

Similarly, to perform the measurement labeled by $y$, Bob measures
an observable with eigenvectors \(|b\rangle\rangle (b = 0, 1, \ldots, d−1,\) and \(y = 1, 2, \ldots, m,\) and

\[
|b\rangle\rangle = \frac{1}{\sqrt{d−1}} \sum_{b=0}^{d−2} \exp \left( \frac{-2ni}{d} \beta_y \right) |b\rangle
\]

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

\[
l_{d,m}(\langle |\psi\rangle\rangle) = \sum_{i,j=1}^{m,d−1} \left| \langle \Phi_i | \langle \Phi_j \rangle \right| ^2,
\]

where \(\Phi_i = \sum_{a=0}^{d−1} \omega^a |a\rangle \langle a|, \Phi_j = |\Phi_i\rangle,\) and \(\omega = \exp(2\pi i/d).\) Note that \(\Phi_i\) and \(\Phi_j\) are unitary matrices.

In ref. 23, it was proved that the Tsirelson bound of \(l_{d,m}\) is \(m(d−1),\) which is achieved exactly by \(|\Phi_d\rangle\rangle\) and strictly larger than the classical bound. Indeed, a property of \(|\Phi_d\rangle\rangle\) is that for any \(d \times d\) matrices \(M\) and \(N,\) it holds that \((M \otimes N) |\Phi_d\rangle\rangle = (I \otimes MN) |\Phi_d\rangle\rangle.\)

Since \(\Phi_i = |\Phi_i\rangle\rangle\) for any \(i\) and \(l,\) we have that \(
\langle \Phi_d | \langle \Phi_i \rangle \langle \Phi_j \rangle \rangle = \langle \Phi_d | \langle I \otimes l \rangle \langle I \otimes i \rangle \rangle = 1,
\)

implying that \(l_{d,m} = m(d−1)\) 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., \(U_1 = U_2 = U,\) \((U_1 \otimes U_2) |\Phi_d\rangle\rangle\) always achieve the Tsirelson bound of \(l_{d,m}.\) In fact, for any \(i\) and \(l\) it holds that

\[
\langle \Phi_d | \langle U \otimes U \rangle \rangle \langle \Phi_i | \langle \Phi_j \rangle \rangle = \langle \Phi_d | \langle I \otimes I \rangle \rangle = 1.
\]

Hence, the new value of \(l_{d,m}\) is still \(m(d−1).\) In this situation, similar to the case of single-qubit quantum circuits, we need to consider whether the converse is correct or not, i.e., whether we can have both \(U_1 \neq U_2\) and \(l_{d,m}(U_1 \otimes U_2) |\Phi_d\rangle\rangle = m(d−1)\) at the same time. We now show that this is impossible.

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

**Proof.** We only need to prove that \(l_{d,m}(U_1 \otimes U_2) |\Phi_d\rangle\rangle = m(d−1)\) implies \(U_1 = U_2.\) According to the definition of \(l_{d,m}\) we know that if \(l_{d,m}(U_1 \otimes U_2) |\Phi_d\rangle\rangle = m(d−1),\) each term in the summation of Eq. (6) will be 1. Therefore, for any \(i \in \{1, 2, \ldots, \}\) it holds that (let \(l = 1\))

\[
\langle \Phi_d | \langle U_1 \otimes U_2 \rangle \rangle \langle \Phi_i | \langle \Phi_j \rangle \rangle = \langle \Phi_d | \langle I \otimes I \rangle \rangle \langle \Phi_i | \langle \Phi_j \rangle \rangle = \frac{1}{d} \text{Tr}(U_1 U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle) = 1.
\]

where we have utilized the fact that for any \(d \times d\) matrices \(M\) and \(N,\) it holds that \((M \otimes 1) |\Phi_d\rangle\rangle = (I \otimes MN) |\Phi_d\rangle\rangle.\) Hence, we obtain that \(\text{Tr}(U_1 U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle) = d.\)

Meanwhile, note that \(U_1 U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle^\dagger = \text{Tr}(U_1^\dagger U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle) = I.\)

Similarly, let \(l = 1, 2, \ldots, \) and \(S_1 = U_1 U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle^\dagger \) is a \(d \times d\) unitary matrix, thus we have that \(U_1 U_2^\dagger |\Phi_i\rangle \langle \Phi_j | U_1^\dagger U_2^\dagger \rangle^\dagger = I.\) For simplicity, let \(S_1 = S_2 = I,\) then \(S_1 S_2 S_1 S_2 = I\), which is also \(S_1 = S_2 = I.\) Therefore, 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.

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

**Theorem 2.** Suppose \(V = l_{d,m}(U_1 \otimes U_2) |\Phi_d\rangle\rangle,\) 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 \(|\alpha\rangle = (U_1 \otimes U_2)|\Phi_0\rangle = (I \otimes U_2|U_1\rangle)|\Phi_0\rangle\). Suppose an orthogonal decomposition of \(U_2|U_1\rangle\) is \(\sum_{j=0}^{d-1} d^j|\lambda_j\rangle/\sqrt{d}\). Note that we also have \(|\Phi_d\rangle = \sum_{j=0}^{d-1} |\lambda_j\rangle|\lambda_j\rangle^* / \sqrt{d}\). Therefore, we have that

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

(14)

Let \(|\alpha\rangle = c_1|\Phi_d\rangle + c_2|\Phi_0\rangle\), where \(c_1\) and \(c_2\) are complex numbers, \(|c_1|^2 + |c_2|^2 = 1\), and \(|\Phi_d\rangle = 0\). Then it can be seen that

\[
c_1 = (|\Phi_d\rangle, |\alpha\rangle) = \frac{1}{d} \sum_{j=0}^{d-1} d^j = \text{Tr}(U_2|U_1\rangle) / d.
\]

(15)

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

For convenience, let \(B = \sum_{i=0}^{m} \sum_{j=1}^{d-1} (A_i^X A_j^Z)\). Then it holds that

\[
V = \langle a|B|a\rangle = \langle c_1|\Phi_d\rangle + c_2|\Phi_0\rangle\rangle, \langle B|c_1|\Phi_d\rangle + c_2|\Phi_0\rangle\rangle
\]

\[
= |c_1|^2\langle \Phi_d|\Phi_d\rangle + c_2|\Phi_0\rangle\rangle
\]

\[
= |c_1|^2 \cdot m(d-1) + (1 - |c_1|^2)\langle B|\Phi_0\rangle\rangle.
\]

(16)

According to Lemma 1, we have that

\[
-m \leq \langle B|\Phi_0\rangle\rangle \leq m(d-2),
\]

which means that

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

(17)

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.

To examine the performance of the above analytical bounds, we test them with numerical simulations. For this, we generate many random instances for \(U_1\) and \(U_2\) for each pair of \(U_1\) and \(U_2\), we compute the corresponding exact values of \(D(U_1, U_2)\), which are next compared with the lower and upper bounds for \(D(U_1, U_2)\) given by Theorem 2. The results are listed in Fig. 1, where it can be seen that the lower bound is quite tight in many instances.

**Direct determination of the distance \(D(U_1, U_2)\)**

In Fig. 1, it can be observed that in most cases the upper bound for \(D(U_1, U_2)\) given by Theorem 2 is quite loose compared with the lower bound. From the proof for Theorem 2, it can be seen that the reason is that the bound \(\langle B|\Phi_0\rangle\rangle \leq m(d-2)\) we have utilized is far from tight in most cases. If we could somehow improve the upper bound for \(\langle B|\Phi_0\rangle\rangle\), our estimation for \(D(U_1, U_2)\) will be more accurate accordingly.

To understand the behavior of \(\langle \psi|\Phi\rangle\rangle\), we study its value for a uniformly random pure state \(|\Phi\rangle\rangle\). It turns out that \(\langle \psi|\Phi\rangle\rangle\) is very small with a probability close to 1. Particularly, we have the following fact, and its proof can be seen in Supplementary Note 2.

**Lemma 2.** Given \(0 < \delta < 1\). Suppose \(|\psi\rangle\rangle\) is a d \times d quantum state, which as a unit vector is chosen uniformly at random on the \(d^2\) dimensional real unit sphere. Then with the probability of no less than \(1 - \delta\) it holds that

\[
ld_m(|\psi\rangle\rangle) \leq m \sqrt{\frac{4}{3\delta d}}.
\]

(18)

Though for a random pair \(U_1\) and \(U_2\), it is possible that the distribution of \(|\Phi_0\rangle\rangle\) is not uniformly random, the above lemma still helps us to understand why the estimation \(\langle \Phi_0|B|\Phi_0\rangle\rangle \leq m(d-2)\) is quite loose overall. Inspired by this, we now adjust the structure of our protocol, and the purpose is to make sure that the new value of \(\langle \Phi_0|B|\Phi_0\rangle\rangle\) is low.

Suppose \(U_1\) and \(U_2\) are the two n-qubit circuits that we want to compare. Now we construct a 2n-qubit circuit as shown in Fig. 2, and denote it as \(U_n\), where \(U_1\) is a part of \(U_n\). And \(U_n\) is constructed similarly. Then we apply our protocol to compare the new quantum circuits \(U_n\) and \(U_n\), whose size is now larger.

We now prove that this adjustment will pin down the new value of \(\langle \Phi_0|B|\Phi_0\rangle\rangle\) to be \(-m\), which is actually the smallest possible. As a result, the upper bound for \(D(U_n, U_n)\) given by Theorem 2 now matches the lower bound completely. That is to say, from the value of Bell expression \(ld_m((U_n \otimes U_n)|\Psi_d\rangle\rangle)\), \(D(U_n, U_n) = D(U_n, U_n)\) can be determined directly, where \(d = 2^{2n}\).

**Theorem 3.** Suppose \(V = ld_m((U_n \otimes U_n)|\Psi_d\rangle\rangle)\) where \(d = 2^{2n}\), then we have that

\[
D(U_n, U_n) = D(U_n, U_n) = \sqrt{1 - \frac{V + m}{md^2}}.
\]

(19)

**Proof.** Denote the operation of all the control-Z gates combined in Fig. 2 by \(U_{2n}\) (as a unitary matrix on 2n qubits). That is
$U'_1 = U_2(U_1 \otimes I)$, $U'_2 = U_2(U_2 \otimes I)$. Then
\[
D(U'_1, U'_2) = \sqrt{1 - \frac{1}{2^m} \Tr(U'_1 U'_2)}
\]
\[
= \sqrt{1 - \frac{1}{2^m} \Tr(U'_1 U'_2 U_2^T U_2)}.
\]

(20)

In the proof for Lemma 1 (see Supplementary Note 1), we have already known that if we let $(U'_1 \otimes U'_2) |\Theta_d\rangle = \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} Y_{ij} |k\rangle |j\rangle$, it holds that
\[
l_{d,m}(U'_1 \otimes U'_2) |\Theta_d\rangle = m \left[ \sum_{k=0}^{d-1} \left( \sum_{j=0}^{d-1} Y_{ij}^2 \right)^2 + \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} Y_{k, j-r} |k\rangle |j\rangle \right] - m.
\]
(21)

Now let us notice the following properties of $Y_{ij}$. Let $k = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_n$ and $j = c_1 c_2 \ldots c_n d_1 d_2 \ldots d_n$ be binary representations of $k$ and $j$, where $a_0, b_0, c_0, d_0 \in \{0, 1\}$ for $1 \leq i \leq n$. Then based on the construction of $U'_1$ and $U'_2$ given by Fig. 2, it can be verified that
1. If $a_1 a_2 \ldots a_n = c_1 c_2 \ldots c_n$, then $Y_{ij} = 0$;
2. If $a_1 a_2 \ldots a_n = c_1 c_2 \ldots c_n$ and $b_i \neq d_i$, we let $k' = a_1 a_2 \ldots a_{i-1} (1 - a_i) a_{i+1} \ldots a_n b_1 b_2 \ldots b_n$ and $j' = c_1 c_2 \ldots c_{i-1} (1 - a_i) c_{i+1} \ldots c_n d_1 d_2 \ldots d_n$, where $Y_{k', j'} = -Y_{ij}$, which have utilized the facts that only one of $a_i$ and $1 - a_i$ can trigger the $Z$ operators on the positions $b_i$ and $d_i$, and that $b_i \neq d_i$.

By using the properties repeatedly, one can prove that
\[
l_{d,m}(U'_1 \otimes U'_2) |\Theta_d\rangle = m \left[ \sum_{k=0}^{d-1} \sum_{j=0}^{d-1} Y_{ij}^2 \right] - m
\]
(22)

$D(U'_1, U'_2) = \sqrt{1 - \frac{1}{2^m} l_{d,m}}$.

Therefore, to determine the distance between two $n$-qubit quantum circuits, we can embed them into two larger $2n$-qubit quantum circuits and then apply our original protocol to the latter. Though the cost is a little bit higher, the estimation for the distance can be much more accurate. We also perform numerical simulations to verify our modified protocol, where again random $U_1$ and $U_2$ are sampled. The results are listed in Fig. 3.

The analysis of computational cost

Now let us analyze the computational cost of our modified protocol, that is, the number of times that we have to run the unknown circuits in order to give a good estimation of the distance $D(U_1, U_2)$ based on Theorem 3. For convenience, we reformulate the Bell expression as below, and the corresponding details can be found in\textsuperscript{11}.
\[
l_{d,m} = dm l_{d,m} - m
\]
\[
l_{d,m} = \frac{d-1}{m} \sum_{k=0}^{d-1} \sum_{i=1}^{m} \alpha_k \left[ P(A_i = B_i + k) + P(B_i = A_i + k) \right]
\]
(23)

where $\alpha_k = \frac{1}{2^m} \tan \left( \frac{\pi}{2^m} \right) \cot \left( \frac{\pi}{2^m} \right) (k + \frac{1}{2^m})$ and $A_m, 1 = A_1 + 1$. For simplicity, in this section $l_{d,m}$ and $l'_{d,m}$ are short for $l_{d,m}(U_1 \otimes U_2) |\Psi_d\rangle$ and $l'_{d,m}(U_1 \otimes U_2) |\Psi_d\rangle$, respectively. Since $-m \leq l_{d,m} \leq m(d-1)$, we have $0 \leq l'_{d,m} \leq 1$. Meanwhile, Theorem 3 implies that $D(U_1, U_2) = \sqrt{1 - l'_{d,m}}$.

Now we consider the estimation of $l'_{d,m}$, where $d = 2^m$. First Alice and Bob apply circuits on their own subsystems of the maximally entangled state to get $(U'_1 \otimes U'_2) |\Psi_d\rangle$. Then choose $r \in \{0, 1\}$ and $i \in \{1, 2, \ldots, m\}$ equiprobably. If $r = 0$, Alice and Bob perform measurements $A_i$ and $B_i$ respectively and obtain the outcomes $a$ and $b$, then they return $2a \mod d$. If $r = 1$, Alice and Bob perform measurements $A_{i+1}$ and $B_i$ and obtain the outcomes $a$ and $b$, then they return $2a \mod d$. They repeat the above process $s$ times. Denote the return values by $X_s$, $j = 1, 2, \ldots, s$. Then it turns out that $X_s \equiv \sum_{j=0}^{s-1} X_j \mod d$. Indeed, note that $E(X_s) = l'_{d,m}$, which means $E(X) = l'_{d,m}$. Furthermore, since $|\alpha_k| \leq 1$, by Hoeffding’s inequality, if $s > 8 \log (1/\delta) / \epsilon^2$, we have that
\[
P(X - l'_{d,m}) \geq \epsilon \leq \delta.
\]
(24)

That is to say, in order to estimate the value of $l'_{d,m}$ within additive error $\epsilon$, the cost of our protocol is $O(\log (1/\delta)/\epsilon^2)$, which is completely independent of the dimension. Then according to Theorem 3, if we want to estimate $D = D(U_1, U_2)$ within additive error $\epsilon$, then the cost of our protocol will be $O(\log (1/\delta)/D^2 \epsilon^2)$ if $D > \epsilon$, or $O(\log (1/\delta)/\epsilon^3)$ if $0 \leq D \leq \epsilon$.

As a comparison, we can consider an alternative approach to verify whether $U_1$ and $U_2$ are the same, which performs quantum process tomography (QPT) for $U_1$ and $U_2$ separately and then compare the two outputs. The standard QPT technique needs to estimate roughly $O(d^4)$ quantities. Recently, QPT protocols have been customized to characterize unitary operations\textsuperscript{23,24,25}, which reduced the cost to $O(d^2)$. The cost of our protocol is much less than QPT and gets rid of the exponential growth with the number of qubits increasing, which means our protocol is practical in the era of large-scale quantum computation.

Lastly, we would like to stress that the measurements involved in our protocol can be physically implemented by a series of single-qubit measurements. In fact, it is not hard to verify that the observable eigenvectors given in Eqs. (4) and (5) can always be decomposed as tensor products of single-qubit pure states as below:
\[
|a\rangle_x = \sum_{k=0}^{d-1} \frac{1}{\sqrt{d}} \exp \left[ \frac{\pi i k}{d} (a - a_x) \right] |k\rangle
\]
\[
= \bigotimes_{j=1}^{d} \left( |0\rangle + \exp \left[ \frac{\pi i k}{d} (a - a_x) \right] |1\rangle \right) / \sqrt{2}.
\]
(25)

As a result, to measure the original observables characterized by Eqs. (4) and (5), one only needs to measure the quantum system qubit by qubit, from $j = n$ to $j = 1$, which can obtain the original measurement outcome bit by bit. This implies that it is realistic to implement our protocol physically.

The equivalence checking of multiple quantum circuits

Now let us go one step further. Suppose we have $k \geq 3$ quantum circuits $C_1, C_2, \ldots, C_n$ and again we want to know whether they are equivalent to each other. Apparently, we can solve the problem by comparing these quantum circuits pair by pair. But if we are unlucky, we need to run the above two-circuit protocol for $k-1$
times. With the success in the two-circuit case, we may wonder, whether or not we can design a similar protocol such that a proper $k$-partite Bell inequality allows us to solve the multi-circuit problem in one go. We now show that, at least in the case that $k$ is odd, this is impossible.

Recall that a key part of our protocol is finding a $k$-partite quantum state $\psi_{ki}$ and a certain Bell inequality such that $\psi_{ki}$ violates it maximally. Furthermore, $\psi_{ki}$ has to satisfy the condition that for any local unitary matrix $U$, it holds that $(U \otimes U \otimes \cdots \otimes U)|\psi_k\rangle = |\psi_k\rangle$.

For simplicity, we now suppose that for each party the local dimension is 2, and the following argument is easy to be generalized to high-dimensional cases. Then we have that

$$(\sigma_x \otimes \sigma_x \otimes \cdots \otimes \sigma_x)|\psi_k\rangle = |\psi_k\rangle$$

and

$$(\sigma_z \otimes \sigma_z \otimes \cdots \otimes \sigma_z)|\psi_k\rangle = |\psi_k\rangle,$$

where $\sigma_x$ and $\sigma_z$ are Pauli matrices. However, since $k$ is odd, $\sigma_x \otimes \sigma_x \otimes \cdots \otimes \sigma_x$ and $\sigma_z \otimes \sigma_z \otimes \cdots \otimes \sigma_z$ anticommute, which means that $|\psi_k\rangle$ is the zero vector, a contradiction. Therefore, when $k$ is odd, we cannot generalize our two-circuit protocol to solve the equivalence checking problem in one go. However, we cannot rule out this possibility for the case that $k$ is even, where the major challenge is to find a desirable multipartite Bell inequality. We leave this for future work.

**DISCUSSION**

In this paper, we have proposed a protocol for black-box 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, we have shown that for any given strength of observed quantum nonlocality, the distance between two compared quantum circuits can be estimated accurately in an analytical manner. Furthermore, it turns out that the computational cost of our protocol is independent of the size of compared quantum circuits. Our work can be regarded as a nontrivial application of quantum nonlocality in the area of quantum engineering, and we hope this protocol can be applied in future quantum industries.

**DATA AVAILABILITY**

The data that support this study are available at https://github.com/sunwx17/Equivalence-checking.

**CODE AVAILABILITY**

The code that supports this study are available at https://github.com/sunwx17/Equivalence-checking.

Received: 28 March 2022; Accepted: 10 November 2022; Published online: 29 November 2022

**REFERENCES**

1. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. Nature **574**, 505–510 (2019).
2. Zhong, H.-S. et al. Quantum computational advantage using photons. Science **370**, 1460–1463 (2020).
3. Viamontes, G. F., Markov, I. L. & Hayes, J. P. Checking equivalence of quantum circuits and states. In 2007 IEEE/ACM International Conference on Computer-Aided Design, 69–74 (IEEE, 2007).
4. Yamashita, S. & Markov, I. L. Fast equivalence-checking for quantum circuits. In 2010 IEEE/ACM International Symposium on Nanoscale Architectures, 23–28 (IEEE, 2010).
ACKNOWLEDGEMENTS

We thank the anonymous referees for their valuable comments. This work was supported by the National Key R&D Program of China, Grants Nos. 2018YFA0306703, 2021YFE0113100, and the National Natural Science Foundation of China, Grant Nos. 61832015, 62272259.

AUTHOR CONTRIBUTIONS

Z.W. conceived the idea of this paper and supervised the project. W.S. analyzed and optimized the protocol. Z.W. and W.S. wrote the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-022-00652-x.

Correspondence and requests for materials should be addressed to Zhaohui Wei.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

© The Author(s) 2022