ARTICLE OPEN

Check for updates

Equivalence checking of quantum circuits by nonlocality

Weixiao Sun [1] and Zhaohui Wei [2,3]✉

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.

npj Quantum Information (2022)8:139 ; https://doi.org/10.1038/s41534-022-00652-x

INTRODUCTION

In the past several years, physical realizations of quantum computing have achieved remarkable progresses[1,2]. 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. [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 ref. [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 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[5–10]. Very recently, equivalence checking has also been introduced to handle sequential quantum circuits, where a Mealy machine-based framework was proposed[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 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[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 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

[1]Institute for Interdisciplinary Information Sciences, Tsinghua University, 100084 Beijing, China. [2]Yau Mathematical Sciences Center, Tsinghua University, 100084 Beijing, China. [3]Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, 101407 Huairou, China. ✉email: weizhaohui@gmail.com

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 computational 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[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 ±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., $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. 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 σ_X and σ_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 $\langle A_x B_y\rangle = \sum_{a,b} ab \cdot p(ab|xy)$, and

$$I_{\mathrm{CHSH}} = \langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_0 B_1\rangle - \langle A_1 B_1\rangle, \tag{1}$$

then it holds that $I_{\mathrm{CHSH}} = 2\sqrt{2}$. 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 of 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 $|\psi\rangle = \frac{1}{\sqrt{2}}(U_1|0\rangle \otimes U_2|0\rangle + U_1|1\rangle \otimes U_2|1\rangle)$, 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_{CHSH}, denoted I'_{CHSH}.

We first consider the case that $U_1 = U_2$. Recall that they are real unitary matrices, then it can be verified that $|\psi\rangle = |\mathrm{EPR}\rangle$, which means $I'_{\mathrm{CHSH}} = 2\sqrt{2}$. 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 $I'_{\mathrm{CHSH}} = 2\sqrt{2}$ 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 $I'_{\mathrm{CHSH}} = 2\sqrt{2}$, the following conditions are satisfied[17].

$$\frac{A_0 \pm A_1}{\sqrt{2}}|\psi\rangle = B_{0/1}|\psi\rangle. \tag{2}$$

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

$$|\Phi_d\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle. \tag{3}$$

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, where 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 $p(ab|xy)$, 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. 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–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 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. [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

$$|a\rangle_x = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp\left[\frac{2\pi \mathbf{i}}{d}k(a - \alpha_x)\right]|k\rangle, \tag{4}$$

where $\mathbf{i} = \sqrt{-1}$ is the imaginary number, and $\alpha_x = (x - 1/2)/m$. Similarly, to perform the measurement labeled by y, Bob measures

an observable with eigenvectors $|b\rangle_y$ ($b=0,1,\ldots,d-1$, and $y=1,2,\ldots,m$), and

$$|b\rangle_y=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp\left[-\frac{2\pi\mathbf{i}}{d}k(b-\beta_y)\right]|k\rangle, \tag{5}$$

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

$$I_{d,m}(|\phi\rangle)=\sum_{i=1}^{m}\sum_{l=1}^{d-1}\langle\phi|(A_i^l\otimes\overline{B}_i^l)|\phi\rangle, \tag{6}$$

where $A_i^l=\sum_{a=0}^{d-1}\omega^{al}|a\rangle_{ii}\langle a|$, $\overline{B}_i^l=(A_i^l)^*$, and $\omega=\exp(2\pi\mathbf{i}/d)$. Note that A_i^l and $\overline{B}_i^l$ are unitary matrices.

In ref. [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 $(M\otimes N)|\Phi_d\rangle=(I\otimes NM^T|\Phi_d\rangle)$. Since $\overline{B}_i^l=(A_i^l)^*$ for any i and l, we have that $\langle\Phi_d|(A_i^l\otimes\overline{B}_i^l)|\Phi_d\rangle=\langle\Phi_d|(I\otimes I)|\Phi_d\rangle=1$, 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 achieve the Tsirelson bound of $I_{d,m}$. In fact, for any i and l it holds that

$$\begin{aligned}&\langle\Phi_d|(U^{\mathsf{T}}\otimes U^{\mathsf{T}})(A_i^l\otimes\overline{B}_i^l)(U\otimes U)|\Phi_d\rangle\\&=\langle\Phi_d|(I\otimes U^{\mathsf{T}}\overline{B}_i^lUU^{\mathsf{T}}(A_i^l)^{\mathsf{T}}U)|\Phi_d\rangle\\&=\langle\Phi_d|(I\otimes I)|\Phi_d\rangle\\&=1.\end{aligned} \tag{7}$$

Hence, the new value of $I_{d,m}$ 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 $I_{d,m}((U_1\otimes U_2)|\Phi_d\rangle)=m(d-1)$ at the same time. 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. (6) will be 1. Therefore, for any $i\in\{1,2,\ldots,m\}$ it holds that (let $l=1$)

$$\begin{aligned}&\langle\Phi_d|(U_1^{\mathsf{T}}\otimes U_2^{\mathsf{T}})(A_i^1\otimes\overline{B}_i^1)(U_1\otimes U_2)|\Phi_d\rangle\\&=\langle\Phi_d|(I\otimes U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}}U_1)|\Phi_d\rangle\\&=\tfrac{1}{d}\mathrm{Tr}(U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}}U_1)\\&=\tfrac{1}{d}\mathrm{Tr}(U_1U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}})\\&=1,\end{aligned} \tag{8}$$

where we have utilized the fact that for any $d\times d$ matrices M and N, it holds that $\langle\Phi_d|(I\otimes M)|\Phi_d\rangle=\mathrm{Tr}(M)/d$ and $\mathrm{Tr}(MN)=\mathrm{Tr}(NM)$. Hence, we obtain that $\mathrm{Tr}(U_1U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}})=d$.

Meanwhile, note that $U_1U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}}$ is a $d\times d$ unitary matrix, thus we have that $U_1U_2^{\mathsf{T}}\overline{B}_i^1U_2U_1^{\mathsf{T}}(A_i^1)^{\mathsf{T}}=I$. For simplicity, let $S_1=U_2U_1^{\mathsf{T}}$ and $S_2=\overline{B}_i^1$. Then this means $S_1^\dagger S_2S_1S_2^\dagger=I$, which is also $S_2S_1=S_1S_2$, 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 $j\neq i\in\{1,2,\ldots,m\}$ and $S_3=\overline{B}_j^1$, then S_1 and S_3 can also be simultaneously diagonalizable. Recall the definition of $\overline{B}_j^1$, whose eigenvectors are given by the conjugate of Eq. (4), then we have that S_1 can be diagonalized in the following two different ways:

$$S_1=\sum_{a=0}^{d-1}g_a(|a\rangle_{ii}\langle a|)^*=\sum_{a=0}^{d-1}h_a(|a\rangle_{jj}\langle a|)^*, \tag{9}$$

where for any a, g_a and h_a are unit complex numbers. Then

$${}_i^*\langle 0|S_1|0\rangle_i^*=g_0=\sum_{a=0}^{d-1}h_a\cdot|{}_i^*\langle 0|a\rangle_j^*|^2. \tag{10}$$

At the same time, for any $a\in\{0,1,\ldots,d-1\}$ it can be verified that $0<|{}_i^*\langle 0|a\rangle_j^*|^2<1$. Combining this with the fact that $\sum_{a=0}^{d-1}|{}_i^*\langle 0|a\rangle_j^*|^2=1$, we obtain that there exists a $\gamma\in[0,2\pi)$ such that $g_0=h_0=\ldots=h_{d-1}=e^{\mathbf{i}\gamma}$, which implies that $S_1=e^{\mathbf{i}\gamma}\cdot I$. 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 $(U_1\otimes U_2)|\Phi_d\rangle$.

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. For example, unitary operations U_1 and U_2 correspond to two different quantum circuits for the same quantum algorithm, hence they are supposed to be the same. However, due to certain mistakes, one of the quantum circuits contains some more quantum gates, which implies that $U_1\neq U_2$. Here for simplicity, we suppose the error in realizing quantum circuits are unitary error. Note that this form of error covers the case that the preparation of $|\Phi_d\rangle$ is also affected by local unitary errors. Our numerical simulations show that more general forms of weak errors that are expressed as quantum operations can also be handled, though it is hard to provide analytical discussions like in the unitary case below.

Since $U_1\neq U_2$, if we do the Bell experiment introduced previously using U_1 and U_2, the Bell expression value $I_{d,m}((U_1\otimes U_2)|\Phi_d\rangle)$ will not be exactly $m(d-1)$. In this situation, an interesting problem is whether or not we can draw any nontrivial conclusions on $D(U_1,U_2)$, the distance between U_1 and U_2, based on the value of $I_{d,m}((U_1\otimes U_2)|\Phi_d\rangle)$. We now show that this is indeed the case, and furthermore, $D(U_1,U_2)$ can be lower and upper bounded analytically.

In this paper, we choose the definition for $D(U_1,U_2)$ given by ref. [22], which is

$$D(U_1,U_2)=\sqrt{1-\left|\frac{1}{d}\mathrm{Tr}(U_1^{\mathsf{T}}U_2)\right|^2}. \tag{11}$$

Meanwhile, we need to use the following key fact (see Supplementary note 1 for its proof).

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

$$-m\leq I_{d,m}(|\psi\rangle)\leq m(d-2). \tag{12}$$

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

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

$$\sqrt{1-\frac{V+m}{md}}\leq D(U_1,U_2)\leq\sqrt{1-\frac{V-m(d-2)}{m}}. \tag{13}$$

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

$$|a\rangle = \sum_{j=0}^{d-1} e^{\mathrm{i}\theta_j}|\lambda_j\rangle|\lambda_j\rangle^*/\sqrt{d}. \tag{14}$$

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

$$c_1 = \langle\Phi_d|a\rangle = \sum_{j=0}^{d-1}\frac{e^{\mathrm{i}\theta_j}}{d} = \frac{\mathrm{Tr}(U_2 U_1^{\mathrm{T}})}{d}, \tag{15}$$

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

For convenience, let $B = \sum_{i=1}^{m}\sum_{l=1}^{d-1}(A_i^l \otimes \overline{B}_i^l)$. Then it holds that

$$\begin{aligned} V &= \langle a|B|a\rangle = (c_1^*\langle\Phi_d| + c_2^*\langle\Phi^\perp|)B(c_1|\Phi_d\rangle + c_2|\Phi^\perp\rangle) \\ &= |c_1|^2\langle\Phi_d|B|\Phi_d\rangle + |c_2|^2\langle\Phi^\perp|B|\Phi^\perp\rangle \\ &= |c_1|^2 \cdot m(d-1) + (1-|c_1|^2)\langle\Phi^\perp|B|\Phi^\perp\rangle. \end{aligned} \tag{16}$$

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

$$\sqrt{\frac{V - m(d-2)}{m}} \le |c_1| \le \sqrt{\frac{V+m}{md}}. \tag{17}$$

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, then 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.

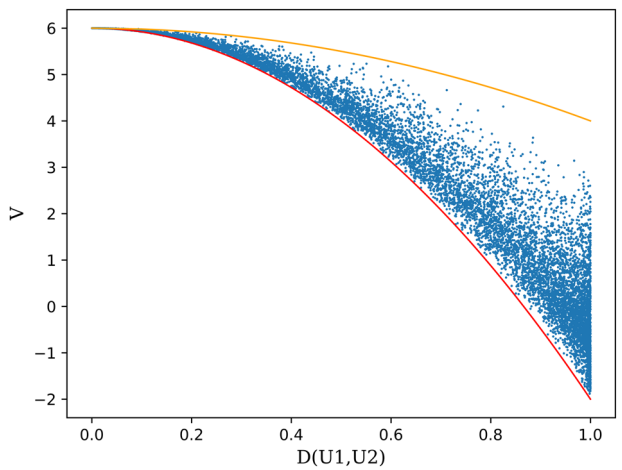

Fig. 1 The values of $D(U_1, U_2)$ and V. Here $d = 4$, $m = 2$, and each blue point represents a pair of U_1 and U_2 that is randomly generated, on which the exact values of $D(U_1, U_2)$ and V are given. The red and the orange solid lines are, respectively, the lower and the upper bounds provided by Theorem 2.

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 $\langle\Phi^\perp|B|\Phi^\perp\rangle \le m(d-2)$ we have utilized is far from tight in most cases. If we could somehow improve the upper bound for $\langle\Phi^\perp|B|\Phi^\perp\rangle$, our estimation for $D(U_1, U_2)$ will be more accurate accordingly.

To understand the behavior of $\langle\phi|B|\phi\rangle$, we study its value for a uniformly random pure state $|\phi\rangle$. It turns out that $\langle\phi|B|\phi\rangle$ 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 $|\psi\rangle$ 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*

$$I_{d,m}(|\psi\rangle) \le m\sqrt{\frac{4}{3d\delta}}. \tag{18}$$

Though for a random pair U_1 and U_2, it is possible that the distribution of $|\Phi^\perp\rangle$ is not uniformly random, the above lemma still helps us to understand why the estimation $\langle\Phi^\perp|B|\Phi^\perp\rangle \le m(d-2)$ 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 $\langle\Phi^\perp|B|\Phi^\perp\rangle$ 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_1', where U_1 is a part of U_1'. And U_2' is constructed similarly. Then we apply our protocol to compare the new quantum circuits U_1' and U_2', whose size is now larger.

We now prove that this adjustment will pin down the new value of $\langle\Phi^\perp|B|\Phi^\perp\rangle$ to be $-m$, which is actually the smallest possible. As a result, the upper bound for $D(U_1', U_2')$ given by Theorem 2 now matches the lower bound completely. That is to say, from the value of Bell expression $I_{d,m}((U_1' \otimes U_2')|\Psi_d\rangle)$, $D(U_1, U_2) = D(U_1', U_2')$ can be determined directly, where $d = 2^{2n}$.

Theorem 3. *Suppose $V = I_{d,m}((U_1' \otimes U_2')|\Phi_d\rangle)$ where $d = 2^{2n}$, then we have that*

$$D(U_1, U_2) = D(U_1', U_2') = \sqrt{1 - \frac{V+m}{md}}. \tag{19}$$

Proof. Denote the operation of all the control-Z gates combined in Fig. 2 by U_Z (as a unitary matrix on $2n$ qubits). That is

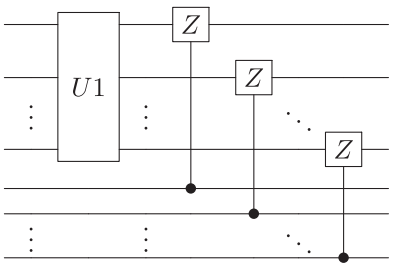

Fig. 2 The $2n$-qubit circuit U_1'. This circuit contains the n-qubit circuit U_1.

$U_1' = U_Z(U_1 \otimes I), U_2' = U_Z(U_2 \otimes I)$. Then

$$\begin{aligned} D(U_1', U_2') &= \sqrt{1 - \left|\tfrac{1}{2^{2n}}\mathrm{Tr}(U_1'^{T} U_2')\right|} \\ &= \sqrt{1 - \left|\tfrac{1}{2^{2n}}\mathrm{Tr}((U_1^{\mathrm{T}} \otimes I) U_Z{}^{\mathrm{T}} U_Z (U_2 \otimes I))\right|} \\ &= \sqrt{1 - \left|\tfrac{1}{2^{2n}}\mathrm{Tr}((U_1^{\mathrm{T}} \otimes I)(U_2 \otimes I))\right|} \\ &= \sqrt{1 - \left|\tfrac{1}{2^{2n}}\mathrm{Tr}(U_1^{\mathrm{T}} U_2 \otimes I)\right|} \\ &= \sqrt{1 - \left|\tfrac{1}{2^{n}}\mathrm{Tr}(U_1^{\mathrm{T}} U_2)\right|} \\ &= D(U_1, U_2). \end{aligned} \tag{20}$$

In the proof for Lemma 1 (see Supplementary Note 1), we have already known that if we let $(U_1' \otimes U_2')|\Phi_d\rangle = \sum_{k=0}^{d-1}\sum_{j=0}^{d-1} \gamma_{kj}|k\rangle|j\rangle$, it holds that

$$I_{d,m}((U_1' \otimes U_2')|\Phi_d\rangle) = m\sum_{r=0}^{d-1}\left(\left|\sum_{k=0}^{d-r-1}\gamma_{k(k+r)}\right|^2 + \left|\sum_{k=d-r}^{d-1}\gamma_{k(k+r-d)}\right|^2\right) - m. \tag{21}$$

Now let us notice the following properties of γ_{kj}. Let $k = a_1a_2\ldots a_nb_1b_2\ldots b_n$ and $j = c_1c_2\ldots c_nd_1d_2\ldots d_n$ be binary representations of k and j, where $a_i, b_i, c_i, d_i \in \{0, 1\}$ for $1 \le i \le n$. Then based on the construction of U_1' and U_2' given by Fig. 2, it can be verified that

1. If $\overline{a_1a_2\ldots a_n} \neq \overline{c_1c_2\ldots c_n}$, then $\gamma_{kj} = 0$;
2. If $\overline{a_1a_2\ldots a_n} = \overline{c_1c_2\ldots c_n}$ and $b_i \neq d_i$, we let $k' = \overline{a_1a_2\ldots a_{i-1}(1-a_i)a_{i+1}\ldots a_nb_1b_2\ldots b_n}$, and $j' = \overline{c_1c_2\ldots c_{i-1}(1-c_i)c_{i+1}\ldots c_nd_1d_2\ldots d_n}$, then $\gamma_{k'j'} = -\gamma_{kj}$, where we 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 $\sum_{k=0}^{d-r-1}\gamma_{k(k+r)} = \sum_{k=d-r}^{d-1}\gamma_{k(k+r-d)} = 0$ when $r \neq 0$. Thus we have that

$$\begin{aligned} I_{d,m}((U_1' \otimes U_2')|\Phi_d\rangle) &= m\left|\sum_{k=0}^{d-1}\gamma_{kk}\right|^2 - m \\ &= md\left|\langle\Phi_d|(U_1' \otimes U_2')|\Phi_d\rangle\right|^2 - m \\ &= md(1 - D(U_1', U_2')^2) - m. \end{aligned} \tag{22}$$

That is, $D(U_1', U_2') = \sqrt{1 - \frac{V+m}{md}}$.

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[21].

$$\begin{aligned} I_{d,m} &= dml_{d,m}' - m \\ l_{d,m}' &= \tfrac{1}{m}\sum_{k=0}^{d-1}\sum_{i=1}^{m}\alpha_k[P(A_i = B_i + k) + P(B_i = A_{i+1} + k)] \end{aligned} \tag{23}$$

where $\alpha_k = \frac{1}{2d}\tan(\frac{\pi}{2m})\cot(\frac{\pi}{d}(k + \frac{1}{2m}))$ and $A_{m+1} = A_1 + 1$. For simplicity, in this section $I_{d,m}$ and $l_{d,m}'$ are short for $I_{d,m}((U_1' \otimes U_2')|\Psi_d\rangle)$ and $l_{d,m}'((U_1' \otimes U_2')|\Psi_d\rangle)$, respectively. Since $-m \le I_{d,m} \le m(d-1)$, we have $0 \le l_{d,m}' \le 1$. 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 $d = 2^{2n}$. 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 $2\alpha_{a-b \bmod d}$. If $r = 1$, Alice and Bob perform measurements A_{i+1} and B_i and obtain the outcomes a and b, then they return $2\alpha_{b-a \bmod d}$. They repeat the above process s times. Denote the return values by $X_j, j = 1, 2, \ldots, s$. Then it turns out that $X \equiv \frac{1}{s}\sum_{j=1}^{s} X_j$ is an estimation of $l_{d,m}'$.

Indeed, note that $\mathbb{E}(X_j) = l_{d,m}'$, which means $\mathbb{E}(X) = l_{d,m}'$. Furthermore, since $|\alpha_k| \le 1$, by Hoeffding's inequality, if $s > 8\log(1/\delta)/\epsilon^2$, we have that

$$P(|X - l_{d,m}'| \ge \epsilon) \le \delta. \tag{24}$$

That is to say, in order to estimate the value of $l_{d,m}'$ within additive error ϵ, 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 ϵ, then the cost of our protocol will be $O(\log(1/\delta)/D^2\epsilon^2)$ if $D > \epsilon$, or $O(\log(1/\delta)/\epsilon^4)$ if $0 \le D \le \epsilon$.

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[23,24], 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 serial 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:

$$\begin{aligned} |a\rangle_x &= \tfrac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp\left[\tfrac{2\pi i}{d}k(a - \alpha_x)\right]|k\rangle \\ &= \bigotimes_{j=1}^{n}\left(|0\rangle + \exp\left[\tfrac{2\pi i}{d}2^{j-1}(a - \alpha_x)\right]|1\rangle\right)/\sqrt{2}, \\ |b\rangle_y &= \tfrac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\exp\left[-\tfrac{2\pi i}{d}k(b - \beta_y)\right]|k\rangle \\ &= \bigotimes_{j=1}^{n}\left(|0\rangle + \exp\left[-\tfrac{2\pi i}{d}2^{j-1}(b - \beta_y)\right]|1\rangle\right)/\sqrt{2}. \end{aligned} \tag{25}$$

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 $k \ge 3$ quantum circuits $C_1, C_2, \ldots, C_k$, 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 $k-1$

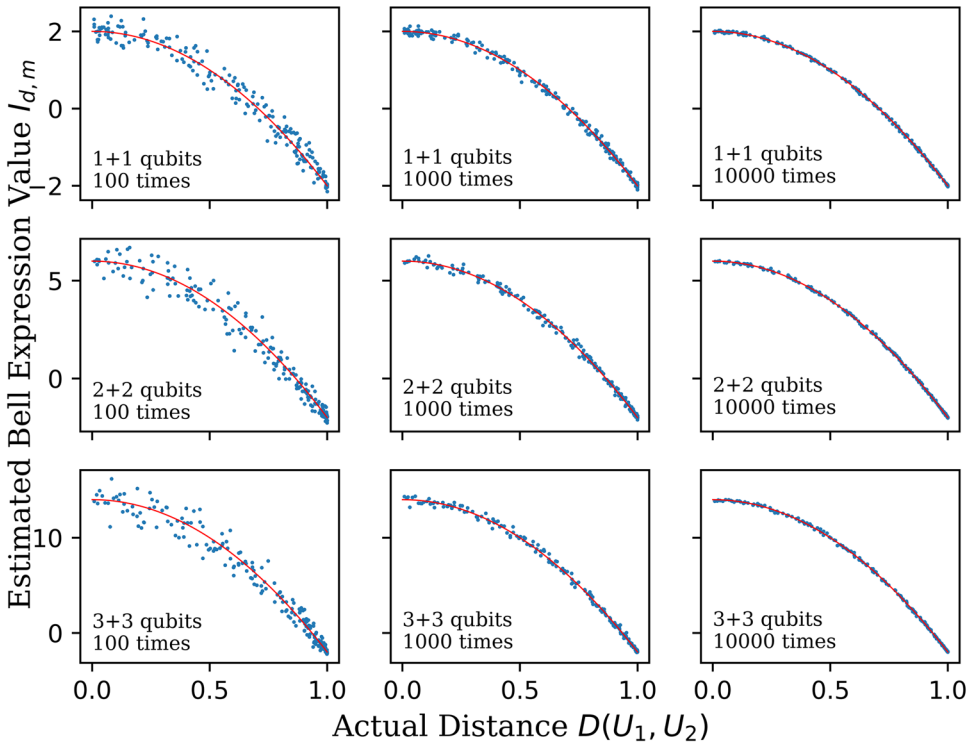

Fig. 3 Determining the distance $D(U_1, U_2)$ based on Theorem 3. Here U_1 and U_2 are randomly sampled, and $m = 2$. Every blue point corresponds to picking up a specific pair of U_1 and U_2 and then running the Monte Carlo process described in section The analysis of computational cost, where $s = 100, 1000, 10{,}000$, respectively. We sample U_1 and U_2 of 1, 2, or 3 qubits, which means the experiments are performed on two 2, 4, or 6-qubit circuits. The red solid line is given by Theorem 3.

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 $|\psi_k\rangle$ and a certain Bell inequality such that $|\psi_k\rangle$ violates it maximally. Furthermore, $|\psi_k\rangle$ 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 σ_x and σ_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).

5. Amy, M., Maslov, D. & Mosca, M. Polynomial-time t-depth optimization of Clifford +T circuits via matroid partitioning. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **33**, 1476–1489 (2014).
6. Nam, Y., Ross, N. J., Su, Y., Childs, A. M. & Maslov, D. Automated optimization of large quantum circuits with continuous parameters. *npj Quantum Inf.* **4**, 23 (2018).
7. Kissinger, A. & van de Wetering, J. Reducing the number of non-Clifford gates in quantum circuits. *Phys. Rev. A* **102**, 022406 (2020).
8. Smith, K. N. & Thornton, M. A. A quantum computational compiler and design tool for technology-specific targets. In *Proc. 46th International Symposium on Computer Architecture*, 579–588 (ACM, 2019).
9. Shi, Y. et al. Certiq: a mostly-automated verification of a realistic quantum compiler. Preprint at https://arxiv.org/abs/1908.08963 (2019).
10. Hietala, K., Rand, R., Hung, S.-H., Wu, X. & Hicks, M. A verified optimizer for quantum circuits. *Proc. ACM Program. Lang.* **5**, 37 (2021).
11. Wang, Q., Li, R. & Ying, M. Equivalence checking of sequential quantum circuits. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **41**, 3143–3156 (2022).
12. Acín, A. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.* **87**, 177901 (2001).
13. D'Ariano, G. M., Lo Presti, P. & Paris, M. G. A. Using entanglement improves the precision of quantum measurements. *Phys. Rev. Lett.* **87**, 270404 (2001).
14. Duan, R., Feng, Y. & Ying, M. Entanglement is not necessary for perfect discrimination between unitary operations. *Phys. Rev. Lett.* **98**, 100503 (2007).
15. Shi, Y. Both Toffoli and controlled-not need little help to do universal quantum computing. *Quantum Inf. Comput.* **3**, 84–92 (2003).
16. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
17. Popescu, S. & Rohrlich, D. Which states violate bell's inequality maximally? *Phys. Lett. A* **169**, 411–414 (1992).
18. Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proc. 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, 503–509 (IEEE, 1998).
19. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
20. Collins, D., Gisin, N., Linden, N., Massar, S. & Popescu, S. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.* **88**, 040404 (2002).
21. Salavrakos, A. et al. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.* **119**, 040402 (2017).
22. Montanaro, A. & Wolf, R. d. *A Survey of Quantum Property Testing. No. 7 in Graduate Surveys* (Theory of Computing Library, 2016).
23. Reich, D. M., Gualdi, G. & Koch, C. P. Minimum number of input states required for quantum gate characterization. *Phys. Rev. A* **88**, 042309 (2013).
24. Baldwin, C. H., Kalev, A. & Deutsch, I. H. Quantum process tomography of unitary and near-unitary maps. *Phys. Rev. A* **90**, 012110 (2014).

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, corrected publication 2022