Verification of Group Non-membership by Shallow Quantum Circuits

Kai Sun, Zi-Jian Zhang, Fei Meng, Bin Cheng, Zhu Cao, Jin-Shi Xu, Man-Hong Yung, Chuan-Feng Li, and Guang-Can Guo

1CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China
2CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China
3Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China
4Department of Computer Science, The University of Hong Kong, Pokfulam, Hong Kong SAR, China
5Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia
6Key Laboratory of Advanced Control and Optimization for Chemical Processes of Ministry of Education, East China University of Science and Technology, Shanghai 200237, China
7Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
8Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
9Shenzhen Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China

Decision problems are the problems whose answer is either YES or NO. As the quantum analogue of NP (nondeterministic polynomial time), the class QMA (quantum Merlin-Arthur) contains the decision problems whose YES instance can be verified efficiently with a quantum computer. The problem of deciding the group non-membership (GNM) of a group element is known to be in QMA. Previous works on the verification of GNM required a quantum circuit with $O(n^2)$ group oracle calls. Here we propose an efficient way to verify GNM problems, reducing the circuit depth to $O(1)$ and the number of qubits by half. We further experimentally demonstrate the scheme, in which two-element subgroups in a four-element group are employed for the verification task. A significant completeness-soundness gap is observed in the experiment.

Introduction—Quantum effect can be used to enhance information processing in many ways. Besides speeding up solving certain problems [1–3], quantum computers can also be used to construct novel interactive proof systems (IPS) [4, 5], which leads to fruitful studies in blind quantum computing [6–8], quantum zero-knowledge proof systems [9, 10] and multiprover interactive proof systems [11, 12], etc. An IPS involves a verifier and (potentially multiple) provers, where the verifier aims at solving certain problems by exchanging messages with the provers.

IPS can be used to classify decision problems, the problems whose answers can only be YES or NO. For example, nondeterministic polynomial time (NP), one of the most important complexity classes, can be described by an IPS, with a classical verifier and a single computationally unbounded prover exchanging one round of classical message [13, 14]. Specifically, NP contains decision problems that, for a YES instance, there exists certain proof message, with which the YES instance can be verified in polynomial time by a classical computer. NP can be generalized to the quantum realm naturally and the quantum analogue is called quantum Merlin-Arthur (QMA) [14, 15]. In QMA, the proof message is replaced by a quantum state and the verifier can use a quantum computer to process it.

Since a classical verifier can be simulated by a quantum computer and a classical message can be described by a quantum state, every problem belongs to NP is also in QMA, i.e., $NP \subseteq QMA$. However, it remains an unsolved problem whether QMA is strictly larger than NP and the group non-membership (GNM) problem is believed to be a feasible candidate that falls in QMA but not in NP [15–18]. Previous works have shown potential quantum advantage on verifying YES instances of this problem. It has been proven that the GNM problem is not in $NP^B$ [17] for a certain group oracle $B$. Also, Watrous proved $GNM(B) \in QMA^B$ for every $B$ by giving quantum proofs and a verification process which can be efficiently done by a quantum computer [18]. Furthermore, Watrous conjectured that certain quantum proofs, which is similar to the one constructed for proving $GNM(B) \in QMA^B$, can be used in many other decision problems of finite groups, such as the problems of deciding proper subgroups and simple groups [18].

Because of the potential applications of quantum IPS and the growing power of near-term quantum devices [19, 20], it has become a meaningful question that how to make quantum IPS more friendly for near-term quantum devices. The verification of the GNM problem is of special importance as it is closely related to the verification of a wide spectrum of group properties and is expected to have quantum advantage. However, Watrous’s process is not favorable for near-term devices as
it requires too deep quantum circuits [18, 21].

In this work, we proposed a new verification process which is more friendly to near-term quantum devices based on Watrous’s protocol. The depth of quantum circuit is reduced to \(O(1)\) for the groups with at most \(2^n\) elements, whereas previous work required \(O(n^5)\) oracle calls in one circuit. The number of qubits needed is also half reduced. Our new process makes it easier to use the verification of GNM as a part of near-term quantum applications such as quantum cryptography protocols. We also demonstrate our new process by an all-optical setup. Various photonic quantum proofs are sent to the optical systems and a significant completeness-soundness gap is presented, showing the validity of our process.

**Group non-membership problem**— First, we formally define the group non-membership problem here [18]. Let \(G\) be a finite group and \(S = \langle g_1, \ldots, g_k \rangle\) be a subgroup generated by group elements \(g_1, \ldots, g_k \in G\). Given an element \(x \in G\), the group non-membership problem is to decide whether \(x\) is outside the subgroup \(S\). If \(x \notin S\), \(x\) is a YES instance; otherwise, \(x\) is a NO instance.

To analyze the problem with minimum assumption on the group, usually the framework of black-box groups [22] is adopted. In this work, we adopt the same framework as in Watrous’s work [18] for the quantum group oracle, in which the quantum group element labels are a set of mutually orthogonal quantum states. We denote the quantum label corresponding to the group element \(g\) by \(|\psi_g\rangle\) and we denote the space spanned by the quantum labels of elements in \(G\) by \(\text{span}\{g\} := \text{span}\{|\psi_{g_1}\rangle, |\psi_{g_2}\rangle : g_1, g_2 \in G\}\). The quantum group oracle is defined to be able to detect whether a state is in \(\text{span}\{G\}\) and carry out right multiplication \(M(\cdot)\) as \(|\psi_g\rangle = |\psi_{g_1g_2}\rangle\).

In Watrous’s process [18], the quantum proof for the non-membership can be a uniform superposition of the elements in a coset \(\alpha S\) of the subgroup \(S\) for any \(\alpha \in G\), where \(\alpha S\) is defined as \(\alpha S := \{\alpha s | s \in S\}\). Explicitly, it can be written as,

\[
|Q_{\text{proof}}\rangle = \frac{1}{\sqrt{|S|}} \sum_{g \in \alpha S} |\psi_g\rangle,
\]

where \(|S|\) is the element number of the subgroup \(S\). This state is invariant under right multiplications of the elements in \(S\) because they map the elements in \(\alpha S\) bijectively to \(\alpha S\). On the other hand, if \(x \notin S\), the result state is orthogonal to the original one as \(\langle Q_{\text{proof}} | M(x) | Q_{\text{proof}} \rangle = 0\) since \((\alpha S)x\) and \(\alpha S\) do not share common elements.

Next, we introduce the core quantum circuit that plays a central role in the verification process. The core circuit is similar to the swap test circuit and is depicted in Fig. 1. The outcome of the core circuit is defined to be the measurement outcome of the control qubit. We denote by \(\text{core}(x, |Q_{\text{proof}}\rangle) = s\) the event of obtaining the measurement outcome \(s \in \{0, 1\}\) in one run of the core circuit with input state \(|Q_{\text{proof}}\rangle\) and group member \(x\). The outcome can show the effect of the multiplication by \(x\) on the input state. For \(\text{core}(x, |Q_{\text{proof}}\rangle)\), if \(x \in S\), the outcome can only be 0 as \(|Q_{\text{proof}}\rangle\) is invariant under the multiplication. If \(x \notin S\), the probability of obtaining 1 is 0.5 as the state after multiplication is orthogonal to \(|Q_{\text{proof}}\rangle\). Therefore, with the proof state, the non-membership of an element can be verified when the outcome 1 is obtained.

However, a malicious prover may send bogus proof states that deviate from Eq. (1) and give incorrect outcomes. Therefore, to ensure the soundness of verification, the verifier has to do a property checking on the received proof state, i.e., check the state is invariant under the quantum multiplication \(\mathcal{M}(s)\) for any \(s \in S\), so that the elements in \(S\) cannot be proven to be outside \(S\). In the original process [18], to verify the proof received is valid, the verifier needs to uniformly sample the subgroup elements in a reversible way and produce a quantum superposition of the quantum labels

\[
\sum_{g \in S} a_i |g\rangle |\text{garbage}(g)\rangle,
\]

where \(\{a_i\}\) should be nearly uniform. However, the reversible sampling requires \(O(n^5)\) calls of the group oracle in the quantum circuit according to Remark 8.3 in [21] and requires the verifier to keep at least one more quantum group element label.

**Simplified verification**— In this work, we reduce both the circuit depth and qubit number needed for the verification of GNM. The simplification relies on the technique which we call Random State Inspection (RSI). RSI can be used in verification processes that includes a property checking phase of the proof state. Usually, in these processes the property checking and the after verification (verification after property ensured) are done in one quantum circuit. Watrous’s process is such a process. In Watrous’s process, the verifier first ensures that the received proof state is invariant under multiplication with subgroup members by multiplying it with the state in Eq. (2) and then carries out the verification with the core circuit. RSI provides a way to reduce the circuit depth by separating the property checking and the verification after property checking.
In RSI, the prover is required to send \( m \) registers that carry copies of a state to the verifier. The verifier randomly selects one register to reserve and apply independent test channels to the other \( m - 1 \) registers to check the property of the states that they carry. If all the \( m - 1 \) registers pass the property checking, the verifier accepts the reserved register for the later verification process. Otherwise, the verifier rejects. We prove that, if all the other registers have passed the test channel, the probability for the reserved register to fail passing the test channel if tested can be bounded to 0 at speed \( O(1/m) \) even when the \( m \) registers are entangled. The verifier can then directly apply the after verification on the reserved register as its property is ensured. By RSI, the circuit depth needed in the verification is reduced to that of the property checking or the after verification.

More important, we simplify the property checking process for the proof state in GNM. Rather than using the state in Eq. (2) which needs \( O(n^5) \) quantum group operations to produce, we propose a test channel in which a subgroup element \( s \) is first classically sampled from a nearly uniform distribution by Babai’s algorithm [21], followed by checking whether \( \text{core}(s, \rho) = 0 \). Here, ‘nearly uniform’ means the probability for \( s \) to be any subgroup elements is in \( (1/|S| - 1/2^{2n}, 1/|S| + 1/2^{2n}) \). We denote the probability for a state \( \rho \) to pass the test channel by \( \Pr(\text{core}(s, \rho) = 0) \). We prove that for any element \( g \in S \) and any quantum state \( \rho \) span \{ \mathcal{O} \}, the probability of incorrectly proving the non-membership of \( g \in S \), i.e. having \( \text{core}(g, \rho) = 1 \), can be bounded as,

\[
\Pr(\text{core}(g, \rho) = 1) \leq 4(1 - \Pr(\text{core}(s, \rho) = 0)) .
\]  

(3)

By RSI, we can ensure \( \Pr(\text{core}(s, \rho) = 0) \) is high enough and therefore bound the error probability \( \Pr(\text{core}(g, \rho) = 1) \).

To summarize, in our new process, we split the property checking of the proof state and the verification after property checking into different circuits by RSI. We also use a new property checking process which requires much less quantum resources. As a result, the verifier only needs to run the core circuits, which is shallow, for many times, rather than run a deep circuit with \( O(n^5) \) group operations. Also, the number of qubits that the verifier needs to keep is halved because the verifier no longer needs to keep the state in Eq. (2). Detailed and rigorous analysis can be found in the supplementary material.

**Experimental setup**—In this work, an experimental demonstration of the our new verification process is carried out. We consider an abelian group \( \mathbb{G} = \{ (A, B)|AB = BA, A^2 = B^2 = E \} \). The four elements in \( \mathbb{G} \) are encoded in the polarization degree of freedom of photons as \( |\psi_E\rangle = |HV\rangle, |\psi_A\rangle = |HV\rangle, |\psi_B\rangle = |HH\rangle \) and \( |\psi_{AB}\rangle = |VV\rangle \), in which \( |H\rangle \) and \( |V\rangle \) denote the horizontal and vertical polarization, respectively. They can together span the whole two-qubit Hilbert space. The optical realization of the controlled right multiplication of \( \{A, B, AB, E\} \) are illustrated in Fig. 2(a). The subgroups we choose are \( S = \{E, A\} \) and \( S' = \{E, AB\} \). The quantum proof states for \( S \) and \( S' \) used in the experiment are \( |Q_{\text{proof}}\rangle = \frac{1}{\sqrt{2}}(|\psi_B\rangle + |\psi_{AB}\rangle) = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \), and \( |Q_{\text{proof}}\rangle = \frac{1}{\sqrt{2}}(|\psi_B\rangle + |\psi_A\rangle) = \frac{1}{\sqrt{2}}(|HH\rangle + |HV\rangle) \), respectively.

In the experimental, we put \( |Q_{\text{proof}}\rangle, |Q_{\text{proof}}\rangle, |\psi_A\rangle \) and \( |\psi_B\rangle \) in the core circuit with right multiplication by \( E, A, B \) and \( AB \). The full experimental setup is shown in Fig. 2(b). The input states are generated by pumping two identically cut type-I beta-barium borate (BBO) crystals whose optic axes are aligned in mutually perpendicular planes [23] with an ultraviolet (UV) source. The UV pulses is frequency doubled from a mode-locked Ti:sapphire laser centered at 800 nm with 130 fs pulse width and 76 MHz repetition rate. After compensating the birefringence effect between \( H \) and \( V \) in BBO crystals with quartz plates (QP), maximally entangled photon pairs of the forms \( |Q_{\text{proof}}\rangle = (|HH\rangle + |VV\rangle)/\sqrt{2} \) are produced [24]. Furthermore, by adjusting the polarization of pump pulses and down-conversion photons, the other states of \( |\psi_B\rangle = |HH\rangle, |\psi_A\rangle = |HV\rangle \) and \( |Q_{\text{proof}}\rangle = (|HH\rangle + |HV\rangle)/\sqrt{2} \) are produced. The input photons are then sent to one of the quantum circuits in Fig. 2 to perform the core circuit with different group multiplications. In our setup, the Mach-Zehnder interferometer is realized by Sagnac interferometer in which the path information of photons is regarded as the control qubit [25]. In a Sagnac interferometer, an optical non-polarization beam splitter (BS), worked as the Hadamard gates on control qubit, is used to separate the beam into two paths 1 and 2 which are treated as the control qubit |0⟩ and |1⟩ respectively. Here, the BS is chosen to split 50 : 50 for 0° angle of incidence which could be decrease the difference of split ratio of different polarizations. In the path |1⟩, a half-wave plate (HWP) is used to implement CNOT gates with set at 45° to reverse the photon polarization. The visibilities of two Sagnac interferometers are 96.7 ± 0.4% and 95.9 ± 0.4%, respectively. Note that, for the circuit \( E \) with \( E \) multiplication, there is no CNOT gate and the HWP is set at 0°. Beams 1 and 2 combine in the BS and then are separated as beams 3 and 4. The polarization of photons are analyzed on the outputs of beams 3 and 4 by polarization beam splitters (PBS), HWP and quarter-wave plates (QWP). The photons are detected by single photon detectors (\( D \)) equipped with 3 nm interference filters (IF).

For the circuit \( A \), which implements the multiplication by \( A \), the probability \( P_0 \) of detecting |0⟩ equals the sum of coincidence count (CC) of detectors located at \( a_3 \) and \( b_3 \) and CC of detectors located at \( a_4 \) and \( b_4 \), where \( a_3 \) is the output port 3 of the SI on the side of \( a \), and similarly hereinafter. The probability \( P_1 \) of detecting |1⟩ equals the sum of CC of \( a_3 \) and \( b_4 \) and CC of \( a_4 \) and \( b_3 \). On
the other hand, for the case of circuit B, according to the corresponding mapping relation where the Sagnac interferometer is only placed in the a side, the probability of detecting $|0\rangle$ equals the CC of $a3$ and $b$, and the probability of $|1\rangle$ equals the CC of $a4$ and $b$. The similar methods suit the other circuits AB and E.

Besides the interference visibility introduced above, two Sagnac interferometers are further verified with the input state of $(|HH\rangle + |VV\rangle)/\sqrt{2}$ which is prepared with a fidelity of $95.9 \pm 1.0\%$. For the Sagnac interferometer appearing in the E circuit, the output state generated from the CC of $a3$ and $b$ remains the maximally entangled state and is achieved experimentally with a fidelity of $95.3 \pm 1.0\%$. For the other interferometer which is used in circuit AB, without inserting the CNOT gate, the output state generated from the CC of $a$ and $b3$ is also the same with the input state and achieves a fidelity of $94.2 \pm 1.4\%$. We further verify other output cases of the interferometers and achieve high fidelities for them. The real and imaginary parts of all corresponding density matrices are presented in the supplementary material.

**Experimental results**— Equipped with the experiment setup, we first carried out our new process on the group $S$. To demonstrate the test channel in our verification process, the correct proof $|Q_{\text{proof}}\rangle$ as well as the bogus proofs $|Q'_{\text{proof}}\rangle$, $|\psi_A\rangle$ and $|\psi_B\rangle$ are produced and sent to the core circuit with multiplication by A. A state passes the test if the control qubit is detected to be in $|0\rangle$. The results are shown in Fig. 3(a). We find that the probabilities for a bogus proof to pass the state test do not exceed $0.518 \pm 0.017$ and have a significant gap towards the probability $0.955 \pm 0.006$ for a correct proof state $|Q_{\text{proof}}\rangle$ to pass. Then we show how the non-membership of an element $g$ can be verified with the correct proof state $|Q_{\text{proof}}\rangle$. The group non-membership of $g$ is verified when $|1\rangle$ is detected in the core circuit with multiplication by $g$. The experimental result is shown in Fig. 3(b). We find the probabilities for $|Q_{\text{proof}}\rangle$ to be accepted is higher than $0.496 \pm 0.009$ for $B, AB \notin S'$ and lower than $0.045 \pm 0.006$ for $E, A \in S'$. The above analysis implies that if the prover sends $m$ registers and the verifier chooses $m - 1$ registers to test, the probability $p_c$ for a group of correct proof state to be accepted is greater than $0.496(0.949)^{m-1}$. In contrast, the probability for $m$ bogus state to pass the tests is only $(0.518)^{m-1}$. For a general bogus proof, our theory shows that the
probability $p_s$ for it to be accepted is bounded by $16/(7(m-1))$. Therefore, the gap $p_c - p_s$ is maximized when $m = 14$ and the maximal value is 0.075.

For the other subgroup $S'$, the result is similar. The bogus proofs become $|\psi_A\rangle$, $|\psi_B\rangle$, $|Q_{\text{proof}}\rangle$, and the correct proof becomes $|Q_{\text{proof}}'\rangle$. The probabilities for the bogus proofs to pass the test channel do not exceed 0.503 ± 0.008 and for the correct proof $|Q_{\text{proof}}'\rangle$, the corresponding probability is 0.980 ± 0.003 as shown in Fig. 3(c). We find that the probability for $|Q_{\text{proof}}'\rangle$ to be accepted when used for verifying GNM is higher than 0.481 ± 0.017 for $B, A \not\in S'$ and is lower than 0.202 ± 0.003 for $E, AB \in S'$ as shown in Fig. 3(d). In this case, $p_s$ is still bounded by $16/(7(m-1))$ and $p_c = 0.481(0.980)^{m-1}$. The gap $p_c - p_s$ is maximized when $m = 19$ and the maximal value is 0.207. These completeness-soundness gaps indicates the success of our experiment.

**Conclusion—** In this work, a new quantum verification process for the GNM problem is proposed, in which the required quantum resources are greatly reduced. We experimentally demonstrate the verification scheme in an all-optical setup. Our novel verification process can be used to construct more quantum protocols for near-term quantum devices. Furthermore, as it is very likely that similar verification process of GNM can be used in other problems of finite groups, it will be interesting if this validity was formally proven and experimentally demonstrated.

**Acknowledgments**

This work was supported by the National Key Research and Development Program of China (Grants NO. 2016YFA0302700 and 2017YFA0304100), National Natural Science Foundation of China (Grant NO. 11821404, 11774335, 61725504, 61805227, 61975195, U19A2075), Anhui Initiative in Quantum Information Technologies (Grant NO. AHY060300 and AHY020100), Key Research Program of Frontier Science, CAS (Grant NO. QYZDYSSW-SLH003), Science Foundation of the CAS (NO. ZDRW-XH-2019-1), the Fundamental Research Funds for the Central Universities (Grant NO. WK2030380017, WK2030380015 and WK2470000026). Natural Science Foundation of Guangdong Province (Grant NO.2017B030308003), the Key R&D Program of Guangdong province (Grant NO. 2018B030326001), the Science, Technology and Innovation Commission of Shenzhen Municipality (Grant NO. JCYJ2017041215260376 and NO. JCYJ2017081710546702 and NO. KYTDPT20181011104202253), National Natural Science Foundation of China (Grant NO. 11875160 and NO. U1801661), the Economy, Trade and Information Commission of Shenzhen Municipality (Grant NO.201901161512), Guangdong Provincial Key Laboratory (Grant NO.2019B121203002).

Z.-J.Z. proposed and proved the theory; K.S. conducted the experiments.

* K.S. and Z.-J.Z. contributed equally to this work.
† jsxu@ustc.edu.cn
‡ yang@sustech.edu.cn
§ cflt@ustc.edu.cn

[1] P. W. Shor, in *Proceedings 35th annual symposium on foundations of computer science* (IEEE, 1994) pp. 124–134.
[2] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman (Association for Computing Machinery, New York, NY, USA, 2003) p. 59–68.
[3] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” (2002).
[4] S. Goldwasser, S. Micali, and C. Rackoff, SIAM Journal on computing *18*, 186 (1989).
[5] J. Watrous, *Theoretical Computer Science* **292**, 575 (2003).
[6] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, 2009) pp. 517–526.
[7] J. F. Fitzsimons and E. Kashefi, *Physical Review A* **96**, 012303 (2017).
[8] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, *Nature physics* **9**, 727 (2013).
[9] A. Broadbent, Z. Ji, F. Song, and J. Watrous, in *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2016) pp. 31–40.
[10] A. B. Grilo, W. Slofstra, and H. Yuen, in *2019 IEEE 60th
[11] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, arXiv preprint arXiv:2001.04383 (2020).
[12] A. Natarajan and J. Wright, in 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS) (IEEE, 2019) pp. 510–518.
[13] M. Sipser, ACM Sigact News 27, 27 (1996).
[14] A. Y. Kitaev, A. Shen, M. N. Vyalyi, and M. N. Vyalyi, Classical and quantum computation, 47 (American Mathematical Soc., 2002).
[15] J. Watrous, arXiv preprint arXiv:0804.3401 (2008).
[16] L. Babai, in Proceedings of the seventeenth annual ACM symposium on Theory of computing, STOC ’85 (ACM, New York, NY, USA, 1985) pp. 421–429.
[17] L. Babai, SIAM Journal on Discrete Mathematics 5, 88 (1992).
[18] J. Watrous, in Proceedings of the 41st Annual Symposium on Foundations of Computer Science, FOCS ’00 (IEEE Computer Society, Washington, DC, USA, 2000) p. 537.
[19] J. Preskill, Quantum 2, 79 (2018).
[20] 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).
[21] L. Babai, in Proceedings of the twenty-third annual ACM symposium on Theory of computing, STOC ’91 (ACM, New York, NY, USA, 1991) pp. 164–174.
[22] L. Babai and E. Szemerédi, in 25th Annual Symposium on Foundations of Computer Science, 1984. (IEEE, 1984) pp. 229–240.
[23] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A 60, R773 (1999).
[24] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A 60, R773 (1999).
[25] K. Sun, X.-J. Ye, Y. Xiao, X.-Y. Xu, Y.-C. Wu, J.-S. Xu, J.-L. Chen, C.-F. Li, and G.-C. Guo, Npj Quantum Information 4, 12 (2018).
SUPPLEMENTARY MATERIAL

For conciseness, in the supplementary material we use $|g\rangle$ rather than $|\psi_g\rangle$ to denote the quantum label of group element $g$. First we formally give the definition of Random State Inspection (RSI) and the test channel used in our new process here.

**Protocol 1: Random State Inspection**

1. Prover sends $m$ registers to the verifier. The registers should carry the same quantum state.
2. Verifier uniformly randomly reserves one register and applies a test channel $T$ to the other $m-1$ registers. The test channel $T$ should map each register to a one-qubit state, with $|0\rangle$ indicating pass and $|1\rangle$ indicating fail.
3. Verifier measures the outputs of the test channels in the computational basis. The reserved register is accepted if and only if all outcomes are 0.

**Protocol 2: Proof State Test Channel $T$**

1. Verifier uses the group oracle to check whether the state of the register is in span${G}$. If it is the case, output $|1\rangle$.
2. Verifier randomly samples a subgroup element by Babai’s algorithm [21] by a classical computer, with the probability of sampling each element in $(\frac{1}{|S|} - \frac{1}{2\pi}, \frac{1}{|S|} + \frac{1}{2\pi})$. Denote the element sampled by $s$.
3. Verifier applies the core circuit to the register with element $s$ by the group oracle.
4. Verifier gives the control qubit in the core circuit as the output.

With Protocol 1 and Protocol 2, we summarize our new verification process here.

**Protocol 3: Verification of Group Non-membership**

1. Prover sends $m$ registers with state in Eq. (1) to the verifier, trying to prove that the element $g$ in the group $G$ is not in the subgroup $S$ of $G$. There are at most $2^n$ elements in $G$.
2. (The test subroutine) Verifier runs Protocol 1 with test channel $T$ defined in Protocol 2 and obtains the reserved register.
3. (The prove subroutine) Verifier applies the core circuit with $g$ to the reserved register after checking the state of the reserved register is in the space span${G} = \text{span}\{|g_1\rangle\langle g_2| : g_1, g_2 \in G\}$ (the space spanned by the valid labels) by the group oracle. The prover passes this subroutine if the outcome of the core circuit is 1 and the state of the register is found in the valid space span${G}$.
4. The prover passes the verification process if he passes both the test and the prove subroutine.

Note that RSI can achieve its goal even when the registers are mixed and entangled. Therefore, a quantum proof $\rho_s$ can be seen as carried by the registers. To prove the validity of Protocol 3, we need to prove its completeness and soundness. We first prove the completeness of it.

**Theorem 1 (Completeness).** In Protocol 3, if the prover and the verifier are honest, for any group element $g$ not in the subgroup, the probability for the prover to prove the non-membership of $g$ is $\frac{1}{2}$.

**Proof.** In the test subroutine, the honest prover will always pass the test because for a honest proof state $|Q_{\text{proof}}\rangle$, $\Pr(\text{core}(s, |Q_{\text{proof}}\rangle)) = 1$. Then, in the prove subroutine, the copy used in this phase has a probability of $\frac{1}{2}$ to be accepted. This can be proved by observing how the proof state is transformed by the core circuit. The transformation is

$$\frac{1}{\sqrt{|S|}} \sum_{s \in \alpha S} |s\rangle \rightarrow \frac{1}{2\sqrt{|S|}} \left( |0\rangle \sum_{s \in \alpha S} (|s\rangle + |sg\rangle) + |1\rangle \sum_{s \in \alpha S} (|s\rangle - |sg\rangle) \right),$$

where the control qubit is put in the left. The probability to obtain $|1\rangle$ after measuring the control qubit is

$$p = \left\| \frac{1}{2\sqrt{|S|}} \sum_{s \in \alpha S} (|s\rangle - |sg\rangle) \right\|^2.$$
Because when \( g \notin S \), we have \( sg \notin \alpha S \) and because for any two \( s_1, s_2 \in \alpha S, s_1 \neq s_2 \), we have \( s_1g \neq s_2g \), the norm can be easily calculated and we can obtain \( p = \frac{1}{2} \). Therefore, the probability to prove the non-membership of an element \( g \notin S \) is \( \frac{1}{2} \) by Protocol 3.

All the verification processes can be done in polynomial time with a quantum computer. According to Thm. (2), only polynomial number of registers are required. The process of every register is only the core circuit with a random group element. The sampling of random group element can also be efficiently done according to Thm. (3). \( \square \)

Below, we denote \( \rho_r \) as the density matrix of the reserved register. Also, we denote \( (\text{test}(\rho_s) = 1) \) as the event that the prover passes this subroutine and \( (\text{test}(\rho_s) = 0) \) otherwise. In addition, we denote \( (T(\rho_r) = 1) \) as \( \rho_r \) passes the test channel (not the test subroutine). Similarly, we denote \( (\text{prove}(g, \rho_s) = 1) \) as the event that the proof state passes the verification process, and \( (\text{prove}(g, \rho_s) = 0) \) otherwise.

**Theorem 2** (Soundness). For any \( g \in S \), the probability to incorrectly verify its non-membership using Protocol 3 vanishes as,

\[
\Pr(\text{prove}(g, \rho_s) = 1) \leq \frac{8}{m},
\]

for any proof state \( \rho_s \).

**Proof.** In this proof we assume that the quantum proof sent by the prover is always in the valid space \( \text{span}\{G\} = \text{span}\{|g_1 \rangle \langle g_2| : g_1, g_2 \in G\} \) because in Protocol 3 the verifier always check whether the states is in \( \text{span}\{G\} \) before doing any operation on them. After the checking, the quantum proof is either projected to \( \text{span}\{G\} \) or rejected. Therefore, the prover making the quantum proof not in \( \text{span}\{G\} \) will only decrease the probability for it to be accepted.

To prove the non-membership of \( g \), the registers should first pass the test subroutine. By Prop. (1), the probability \( \Pr(\text{test}(\rho_r) = 1) \) for the reserved copy \( \rho_r \) to pass the test is bounded as

\[
\Pr(T(\rho_r) = 1|\text{test}(\rho_s) = 1) \geq 1 - \left( \frac{1}{\Pr(\text{test}(\rho_s) = 1)} - 1 \right) \frac{1}{m - 1}.
\]

By Prop. (2), we know that the high probability to pass the test means low error probability to prove the non-membership. For the reserved copy, provided that the test subroutine has been passed, the probability of incorrectly proving GNM by it can be given by,

\[
\Pr(\text{core}(g, \rho_r) = 1|\text{test}(\rho_s) = 1) \leq \frac{1 - \Pr(T(\rho_r) = 1|\text{test}(\rho_s) = 1)}{K(1 - \frac{|S|}{2^{n+1}})},
\]

where

\[
\frac{1}{K} = 1 - \cos \left( \left| \frac{g}{2} \right| \frac{2}{|g|} \right) \leq 2.
\]

Combining the equations, we can obtain the probability of incorrectly accepting the proof state

\[
\Pr(\text{test}(\rho_s) = 1, \text{core}(g, \rho_r) = 1)
= \Pr(\text{test}(\rho_s) = 1) \cdot \Pr(\text{core}(g, \rho_r) = 1|\text{test}(\rho_s) = 1)
\leq \frac{\Pr(\text{test}(\rho_s) = 1)}{K(1 - \frac{|S|}{2^{n+1}})}(1 - \Pr(T(\rho_r) = 1|\text{test}(\rho_s) = 1))
\leq \frac{\Pr(\text{test}(\rho_s) = 1)}{K(1 - \frac{|S|}{2^{n+1}})} \left( \frac{1}{\Pr(\text{test}(\rho_s) = 1)} - 1 \right) \frac{1}{m - 1}
\leq \frac{1}{K} \left( 1 + \frac{1}{2^{n+1} - 1} \right) \frac{1}{m - 1}
\leq \frac{8}{m}.
\]

\( \square \)
Corollary 1. For the group $G = \{\langle A, B \rangle | AB = BA, A^2 = B^2 = E \}$ used in the experimental demonstration in the main text, the probability to incorrectly verify the non-membership of a subgroup element $g$ except $E$ using Protocol 3 vanishes as,

$$\Pr(\text{prove}(g, \rho_s) = 1) \leq \left(\frac{16}{7}\right) \frac{1}{m-1},$$

for any proof state $\rho_s$.

Proof. The rank of the group elements in $G = \{\langle A, B \rangle | AB = BA, A^2 = B^2 = E \}$ are all 2 except $E$. Therefore $1/K = 2$.

Notice that there are 4 elements in $G$ and $n = 2$, refer to Eq. (10), we have

$$\Pr(\text{test}(\rho_s) = 1, \text{core}(g, \rho_r) = 1) \leq \frac{1}{K} \left(1 + \frac{1}{2^{n+1} - 1}\right) \frac{1}{m-1} = 2\left(1 + \frac{1}{2^{2+1} - 1}\right) \frac{1}{m-1} = \left(\frac{16}{7}\right) \frac{1}{m-1}. \quad (12)$$

Proposition 1. In Protocol 1, the probability $\Pr(T(\rho_r) = 1 | \text{test}(\rho_s) = 1)$ for the reserved register $\rho_r$ to pass the test in the condition that all other registers have passed the tests can be bounded as

$$\Pr(T(\rho_r) = 1 | \text{test}(\rho_s) = 1) \geq 1 - \left(\frac{1}{\Pr(\text{test}(\rho_s) = 1)} - 1\right) \frac{1}{m-1}, \quad (13)$$

where $\Pr(\text{test}(\rho_s) = 1)$ is the overall probability for the registers to pass Protocol 1.

Proof. After applying $T$ to every register in $\rho_s$, we can obtain an $m$-qubit state as

$$T^{\otimes M}(\rho_s) = \sum_{s_1, s_2 \in \{0, 1\}^m} a_{s_1, s_2} |s_1\rangle \langle s_2| . \quad (14)$$

Then we try to bound the probability for passing RSI. For the sake of conciseness, we denote $a_{s, s}$ by $a_s$. Also, we denote the $a_s$ in which $s$ is 0 in every indices except in index $i$ as $a_{i=1}$. We have

$$\Pr(\text{test}(\rho_s) = 1) = \frac{1}{m} \sum_{i=1}^{m} (a_{0^m} + a_{i=1}) = a_{0^m} + \frac{1}{m} \sum_{i=1}^{m} a_{i=1}$$

$$\leq a_{0^m} + \frac{1}{m} (1 - a_{0^m}), \quad (15)$$

and

$$a_{0^m} \geq \frac{m \Pr(\text{test}(\rho_s) = 1) - 1}{m-1}. \quad (16)$$

Decompose the density matrix $\rho_r$ of the reserved register after being applied with channel $T$ as

$$\rho_r = \sum_{s_1, s_2 \in \{0, 1\}^2} r_{s_1, s_2} |s_1\rangle \langle s_2|. \quad (17)$$

According to the definition of the conditional probability $\Pr(A|B) = \Pr(A \cap B) / \Pr(B)$, we have

$$\Pr(T(\rho_r) = 1 | \text{test}(\rho_s) = 1) = \frac{a_{0^m}}{\Pr(\text{test}(\rho_s) = 1)}$$

$$\geq 1 - \left(\frac{1}{\Pr(\text{test}(\rho_s) = 1)} - 1\right) \frac{1}{m-1}. \quad (18)$$

\[ \square \]

Corollary 2. After Protocol 1, if the reserved register is tested, the probability $\Pr(T(\rho_r) = 0, \text{test}(\rho_s) = 1)$ for the reserved register to fail passing the test channel together with that the RSI is not rejected is less than $O(1/m)$. 


Proof. By Prop. (1) we know that
\[ \Pr(T(\rho_r) = 1|\text{test}(\rho_s) = 1) \geq 1 - \frac{1}{\Pr(\text{test}(\rho_s) = 1)} - 1 \frac{1}{m-1}. \] (19)

Easily we can know that
\[ \Pr(T(\rho_r) = 1|\text{test}(\rho_s) = 1) \Pr(\text{test}(\rho_s) = 1) \geq \Pr(\text{test}(\rho_s) = 1) - (1 - \Pr(\text{test}(\rho_s) = 1)) \frac{1}{m-1}. \] (20)

\[ \Pr(T(\rho_r) = 1, \text{test}(\rho_s) = 1) \geq \Pr(\text{test}(\rho_s) = 1) - (1 - \Pr(\text{test}(\rho_s) = 1)) \frac{1}{m-1}, \] (21)

\[ \Pr(T(\rho_r) = 1, \text{test}(\rho_s) = 1) \geq \Pr(\text{test}(\rho_s) = 1) - O(1/m), \] (22)

\[ \Pr(T(\rho_r) = 1, \text{test}(\rho_s) = 1) \geq \Pr(T(\rho_r) = 0, \text{test}(\rho_s) = 1) - O(1/m), \] (23)

\[ \Pr(T(\rho_r) = 0, \text{test}(\rho_s) = 1) \leq O(1/m). \] (24)

\[ \Pr(\text{core}(g, \rho_r) = 1) \leq 1 - \frac{1 - \Pr(T(\rho_r) = 1)}{K(1 - \frac{|S|}{2^{2n}})}, \] (25)

where
\[ \frac{1}{K} = 1 - \cos \left( \frac{|g|}{2} \frac{2}{|g|} \pi \right). \] (26)

Proof. First, if \( g = e \), the verifier can immediately reject the proof since \( e \) is contained in every group. In this case \( \Pr(\text{prove}(g, \rho_s) = 1) = 0 \) and the inequality holds. In this following proof, we assume \( g \neq e \) and therefore \( |g| \neq 1 \).

To prove Eq. (25), we just need to prove it for any pure state \( \rho_r = |\psi\rangle \langle \psi| \), because if this theorem is true for any pure state, then for any mix state \( \rho = \sum_i q_i |i\rangle \langle i| \),

\[ \Pr(\text{core}(g, \rho_r) = 1) = \sum_i q_i \Pr(\text{core}(g, |i\rangle) = 1) \leq \sum_i q_i \frac{1 - \Pr(T(|i\rangle) = 1)}{K(1 - \frac{|S|}{2^{2n}})} = \frac{1 - \Pr(T(\rho_r) = 1)}{K(1 - \frac{|S|}{2^{2n}})}. \] (27)

Therefore, we start to prove this theorem for pure state here. We can extend any pure state \( |\psi\rangle \) as
\[ |\psi\rangle = \sum_{\alpha \in G} \beta_{\alpha} |\alpha\rangle \] (28)

For simplicity, in this proof we denote \( \Pr(\text{core}(g, |\psi\rangle) = 1) \) by \( p(g) \). We want to prove
\[ p(g) \leq \frac{1 - \Pr(T(|\psi\rangle) = 1)}{K(1 - \frac{|S|}{2^{2n}})}. \] (29)
In Protocol 3, the state is tested as

$$\sum_{\alpha \in G} \beta_{\alpha} |\alpha\rangle \rightarrow \frac{1}{2} |0\rangle \sum_{\alpha \in G} \beta_{\alpha} (|\alpha\rangle + |\alpha g\rangle) + \frac{1}{2} |1\rangle \sum_{\alpha \in G} \beta_{\alpha} (|\alpha\rangle - |\alpha g\rangle).$$  \(30\)

The probability for an element \(g \in G\) to be verified by the state is

$$p(g) = \frac{1}{4} \left\| \sum_{\alpha \in G} \beta_{\alpha} (|\alpha\rangle - |\alpha g\rangle) \right\|^2$$

$$= \frac{1}{4} \sum_{\alpha \in G} (|\beta_{\alpha}|^2 + |\beta_{\alpha g^{-1}}|^2 - 2\text{Re}(\beta_{\alpha}^* \beta_{\alpha g^{-1}}))$$

$$= \frac{1}{4} (2 - \sum_{\alpha \in G} 2\text{Re}(\beta_{\alpha}^* \beta_{\alpha g^{-1}})).$$  \(31\)

by which we can obtain

$$\sum_{\alpha \in G} \text{Re}(\beta_{\alpha}^* \beta_{\alpha g^{-1}}) = 1 - 2p(g).$$  \(32\)

Decompose \(G\) by the cosets \(G/S = \\{\alpha S | \alpha \in G\}\), where \(\alpha S = \{\alpha s \mid s \in S\}\). Easily one can find that if \(h \in \alpha S\), \(hS = \alpha S\). By this decomposition we sum up Eq. (32) and obtain

$$\sum_{s \in S} (1 - 2p(s)) = \sum_{s \in S} \sum_{\alpha \in G} \text{Re}(\beta_{\alpha}^* \beta_{\alpha s^{-1}})$$

$$= \text{Re}(\sum_{\alpha \in G} \sum_{s \in \alpha S} \beta_{\alpha}^* \beta_{s})$$

$$= \text{Re}(\sum_{\alpha \in G/S} \sum_{h \in \alpha S} \beta_{h}^* \sum_{s \in h S} \beta_{s})$$

$$= \sum_{\alpha \in G/S} |\sum_{h \in \alpha S} \beta_{h}|^2,$$  \(33\)

and therefore

$$\sum_{s \in S} p(s) = \frac{1}{2} (|S| - \sum_{\alpha \in G/S} |\sum_{h \in \alpha S} \beta_{h}|^2).$$  \(34\)

On the other hand, we want to get the probability \(\text{Pr}(T(|\psi\rangle) = 1)\) for this state to pass the test. Notice that the probability for the state to pass the test by \(s\) is

$$\text{Pr}(\text{core}(s, |\psi\rangle) = 0) = 1 - \text{Pr}(\text{core}(s, |\psi\rangle) = 1) = 1 - p(s).$$  \(35\)

Also, in a test the subgroup element used is randomly sampled by Babai’s algorithm. By Thm. (3) we know that in polynomial time we can sample every subgroup element \(s\) with

$$\text{Pr}(s \text{ is sampled}) \in \left(\frac{1}{|S|} - \frac{1}{2^{2n+1}} \frac{1}{|S|} + \frac{1}{2^{2n}}\right).$$  \(36\)

Therefore we have

$$\text{Pr}(T(|\psi\rangle) = 1) = \sum_{s \in S} \text{Pr}(s \text{ is sampled})(1 - p(s))$$

$$= 1 - \sum_{s \in S} \text{Pr}(s \text{ is sampled})p(s)$$

$$\leq 1 - \left(\frac{1}{|S|} - \frac{1}{2^{2n}}\right) \frac{1}{2} (|S| - \sum_{\alpha \in G/S} |\sum_{h \in \alpha S} \beta_{h}|^2)$$

$$= \frac{1}{2} + \frac{|S|}{2^{2n+1}} + \frac{1}{2}\left(\frac{1}{|S|} - \frac{1}{2^{2n}}\right) \sum_{\alpha \in G/S} |\sum_{h \in \alpha S} \beta_{h}|^2.$$  \(37\)
To give a relation between \( p(g) \) and \( \text{Pr}(T(|\psi\rangle) = 1) \), we want to know the maximum of

\[
f(\vec{\beta}) = \sum_{\alpha S \in G/S} \sum_{h \in \alpha S} |\beta_h|^2
\]

under the condition that

\[
b(\vec{\beta}) = \sum_{\alpha \in G} \text{Re}(\beta_\alpha^* \beta_{\alpha g^{-1}}) = B = 1 - 2p(g)
\]

and

\[
l(\vec{\beta}) = \sum_{h \in G} |\beta_h|^2 = 1.
\]

We should survey more carefully the structure of the coset \( \alpha S \). Define \( \text{cycle}(c, g) \) as \( c\langle g \rangle = \{cg^i | i \in \mathbb{Z}\} \). A coset can be decomposed into disjoint orbits. Let \( \text{CYC}(\alpha S, g) \) be a set of \( c \) such that for any \( c_1, c_2 \in \text{CYC}(\alpha S, g) \), \( \text{cycle}(c_1, g) \neq \text{cycle}(c_2, g) \) if \( c_1 \neq c_2 \); and \( \alpha S = \bigcup_{c \in \text{CYC}(\alpha S, g)} \text{cycle}(c, g) \). By these definition we can further decompose the summation as

\[
\sum_{\alpha \in G} \text{Re}(\beta_\alpha^* \beta_{\alpha g^{-1}}) = \sum_{\alpha S \in G/S} \sum_{c \in \text{CYC}(\alpha S, g)} \sum_{k=1}^{\text{|g|}} \text{Re}(\beta_{cg^{-k+1}}^* \beta_{cg^{-k}}).
\]

Define

\[
f_\alpha(\vec{\beta}) = \sum_{c \in \text{CYC}(\alpha S, g)} \sum_{k=1}^{\text{|g|}} \beta_{cg^{-k}},
\]

\[
b_\alpha(\vec{\beta}) = \sum_{c \in \text{CYC}(\alpha S, g)} \sum_{k=1}^{\text{|g|}} \text{Re}(\beta_{cg^{-k+1}}^* \beta_{cg^{-k}}),
\]

\[
l_\alpha(\vec{\beta}) = \sum_{c \in \text{CYC}(\alpha S, g)} \sum_{k=1}^{\text{|g|}} |\beta_{cg^{-k}}|^2.
\]

Therefore

\[
f(\vec{\beta}) = \sum_{\alpha S \in G/S} \sum_{c \in \text{CYC}(\alpha S, g)} \sum_{k=1}^{\text{|g|}} \beta_{cg^{-k}} |^2 = \sum_{\alpha S \in G/S} |f_\alpha(\vec{\beta})|^2.
\]

We want to know the maximum of \( f_\alpha \) when \( b_\alpha \) and \( l_\alpha \) are fixed. To find out this relationship we first define

\[
o_c(\vec{\beta}) = \sum_{k=1}^{\text{|g|}} |\beta_{cg^{-k}}|^2,
\]

\[
b_c(\vec{\beta}) = \sum_{k=1}^{\text{|g|}} \text{Re}(\beta_{cg^{-k+1}}^* \beta_{cg^{-k}}),
\]

\[
l_c(\vec{\beta}) = \sum_{k=1}^{\text{|g|}} |\beta_{cg^{-k}}|^2.
\]
We need to study the maximum of $o_c$ when $g_c$ and $l_c$ are fixed. Decompose every $\beta_h$ into real part and imaginary part as

$$\beta_h = R_h + iI_h. \quad (49)$$

Therefore

$$l_c(\bar{\beta}) = \sum_{n=1}^{\mid g \mid} |\beta_{cg-n}|^2 = \sum_{n=1}^{\mid g \mid} R_{cg-n}^2 + \sum_{n=1}^{\mid g \mid} I_{cg-n}^2 = l_c^R(\bar{R}) + l_c^I(\bar{I}), \quad (50)$$

$$b_c(\bar{\beta}) = \sum_{n=1}^{\mid g \mid} Re(\beta_{cg-n+1}^* \beta_{cg-n}) = \sum_{n=1}^{\mid g \mid} R_{cg-n+1}^* R_{cg-n} + \sum_{n=1}^{\mid g \mid} I_{cg-n+1}^* I_{cg-n} = b_c^R(\bar{R}) + b_c^I(\bar{I}), \quad (51)$$

$$o_c(\bar{\beta}) = \sum_{n=1}^{\mid g \mid} \beta_{cg-n} = \sum_{n=1}^{\mid g \mid} R_{cg-n} + \sum_{n=1}^{\mid g \mid} I_{cg-n} = o_c^R(\bar{R}) + o_c^I(\bar{I}). \quad (52)$$

By Corollary 3 we know that when $b_c^R$ and $l_c^R$ are fixed,

$$\max o_c^R(\bar{R}) = K\mid g \mid (b_c^R - l_c^R) + \mid g \mid l_c^R = K\mid g \mid (b_c^R + \frac{1-K}{K} l_c^R), \quad (53)$$

where

$$K^{-1} = 1 - \cos\left(\frac{|g|}{2}\frac{2}{|g|}\pi\right). \quad (54)$$

Then we get $\max o_c(\bar{\beta})$ under the condition that $b_c^R(\bar{R}) + b_c^I(\bar{I}) = b_c(\bar{\beta})$ and $l_c^R(\bar{R}) + l_c^I(\bar{I}) = l_c(\bar{\beta})$. That is

$$\max o_c(\bar{\beta}) = \max (o_c^R(\bar{R}) + o_c^I(\bar{I})) = \max \left( K\mid g \mid (b_c^R + \frac{1-K}{K} l_c^R) + K\mid g \mid (b_c^I + \frac{1-K}{K} l_c^I) \right) \quad (55)$$

$$= \max \left( K\mid g \mid (b_c^R + b_c^I + \frac{1-K}{K} (l_c^R + l_c^I)) \right)$$

$$= K\mid g \mid (b_c + \frac{1-K}{K} l_c).$$

Therefore we have

$$\max f_c(\bar{\beta}) \leq \sum_{c \in CYC(aS,g)} \sqrt{\max o_c} = \frac{|S|}{|g|} \sum_{c \in CYC(aS,g)} \frac{|g|}{|S|} \sqrt{\max o_c} \leq \frac{|S|}{|g|} \sqrt{\sum_{c \in CYC(aS,g)} \frac{|g|}{|S|} \max o_c} \leq \sqrt{|S|} \sqrt{\sum_{c \in CYC(aS,g)} K\mid g \mid (b_c + \frac{1-K}{K} l_c)} = \sqrt{K|S|} \sqrt{\sum_{c \in CYC(aS,g)} (b_c + \frac{1-K}{K} l_c)} = \sqrt{K|S|} \sqrt{b_c + \frac{1-K}{K} l_c}.$$
Then
\[
\max f(\vec{\beta}) = \max \sum_{\alpha \in G/S} |f_\alpha(\vec{\beta})|^2 \\
\leq \sum_{\alpha \in G/S} |\max f_\alpha(\vec{\beta})|^2 \\
= \sum_{\alpha \in G/S} K|S|(b_\alpha + \frac{1 - K}{K} l_\alpha) \\
= K|S|(B + \frac{1 - K}{K}) = |S|(KB + 1 - K).
\]

Finally
\[
\Pr(T(\psi) = 1) \leq 1 + \frac{|S|}{2n+1} + \left(1 - \frac{1}{2^{2n}}\right) K|S|(KB + 1 - K) \\
= 1 + |S| + \left(1 - \frac{1}{2^{2n}}\right) K(1 - 2p(g)) \\
= 1 + \frac{|S|}{2^{2n}} Kp(g).
\]

\[\text{Proposition 3.}\]

Let \(R\) be a vector of \(n\) real numbers \((n > 1)\). Under the condition that \(\sum_{i=1}^{n} R_i R_{i+1} = b\) \((R_{n+1} \text{ is defined to be } R_1)\), the maximum of \(O = (\sum_{i=1}^{n} R_i)^2\) is
\[
O = \frac{n}{1 - \cos\left(\frac{n}{2}\right)} (b - 1) + n.
\]

**Proof.** The Lagrangian multiplier of this problem is
\[
F(R, \lambda) = (\sum_{i=1}^{n} R_i)^2 + \lambda_1(\sum_{i=1}^{n} R_i R_{i+1} - b) + \lambda_2(\sum_{i=1}^{n} R_i^2 - 1).
\]

The derivatives should be zero when \(O\) is maximized
\[
\frac{\partial F}{\partial R_k} = 2n \sum_{i=1}^{n} R_i + \lambda_1(R_{k-1} + R_{k+1}) + 2\lambda_2 R_k = 0.
\]

Sum up the derivatives, we have
\[
\sum_{k=1}^{n} \frac{\partial F}{\partial R_k} = 2n (\sum_{i=1}^{n} R_i) + 2\lambda_1 \sum_{i=1}^{n} R_i + 2\lambda_2 (\sum_{i=1}^{n} R_i) = 0
\]
and therefore

\[\lambda_1 + \lambda_2 = -n.\] (64)

In a similar way, we have

\[
\frac{\partial F}{\partial R_k} R_k = 2 \left( \sum_{i=1}^{n} R_i \right) R_k + \lambda_1(R_{k-1} R_k + R_k R_{k+1}) + 2\lambda_2 R_k^2 = 0
\] (65)

and therefore

\[
\sum_{k=1}^{n} \frac{\partial F}{\partial R_k} R_k = 2O + 2\lambda_1 b + 2\lambda_2 = 0.
\] (66)

Also, by Eq. (62), we have

\[\lambda_1(R_{k-1} + R_{k+1}) + 2\lambda_2 R_k = \lambda_1(R_k + R_{k+2}) + 2\lambda_2 R_{k+1},\] (68)

and therefore

\[R_k + (2\frac{\lambda_2}{\lambda_1} - 1)R_{k-1} - (2\frac{\lambda_2}{\lambda_1} - 1)R_{k-2} - R_{k-3} = 0.\] (69)

The formula for each \(R_k\) can be obtained by the characteristic equation

\[x^3 + \Lambda x^2 - \Lambda x - 1 = 0,\] (70)

where

\[\Lambda = (2\frac{\lambda_2}{\lambda_1} - 1).\] (71)

The solutions are

\[x = 1, \pm \sqrt{\left(\frac{\lambda_2}{\lambda_1}\right)^2 - 1 - \frac{\lambda_2}{\lambda_1}}.\] (72)

Denote the latter two solutions as \(X_+\) and \(X_-\). Easily, one can verify that we can define \(X\) as \(X_+ = X_-^{-1} = X\). We first point out the relation of \(X\) and \(\lambda_1\) here. By Eq. (72), we have

\[\lambda_1 = \frac{2nX}{(X - 1)^2}.\] (73)

Then, combining with Eq. (67), we obtain

\[O = \lambda_1(1 - b) + n = \frac{2nX}{(X - 1)^2} (1 - b) + n.\] (74)

**When \(n\) is even:**

First, easily one can prove that \(O = 0\) when \(b = -1\), which is denoted by \(O(-1) = 0\). When \(b = -1\), if any \(|R_i|\) is not equal to \(|R_{i+1}|\), by rearrangement inequity we have

\[\sum_i |R_i||R_{i+1}| < \sum_i |R_i||R_i| = 1\] (75)

and

\[b = \sum_i R_i R_{i+1} > - \sum_i |R_i||R_{i+1}| = -1,\] (76)
which is contradictory to our assumption that \( b = -1 \). Therefore, we must have \( |R_i| = |R_{i+1}| \) and easily one can find that \( R_i = -R_{i+1} \) to make \( b = -1 \). Then, \( O(-1) = (\sum_i R_i)^2 = 0 \) when \( n \) is even. Finally we have

\[
O(-1) = 0 = \frac{4nX}{(X-1)^2} + n. \tag{77}
\]

Solving this we have \( X = -1 \), and then \( \lambda_1 = -n/2 \). Therefore,

\[
O = \frac{n}{2} (b - 1) + n = \frac{n}{1 - \cos(\pi/2)} (b - 1) + n = \frac{n}{1 - \cos(\pi/2)} (b - 1) + n. \tag{78}
\]

**When \( n \) is odd:**

We first assume \( X_+ \neq X_- \) and therefore \( X \neq \pm 1 \). The formula for \( R_k \) in this case should be

\[
R_k = A_1 + A_2 X^k + A_3 X^{-k}, \tag{79}
\]

where \( A_1, A_2 \) and \( A_3 \) are parameters that should be determined. Plug Eq. (79) into Eq. (62) and notice that \( X_+ + X_- = -2\lambda / \lambda_1 \), we have

\[
0 = 2 \sum_{k=1}^{n} R_k + \lambda_1 (A_1 + A_2 X^{k-1} + A_3 X^{-(k+1)} + A_1 + A_2 X^{k+1} + A_3 X^{-(k-1)}) + 2\lambda_2 R_k
\]

\[
= 2 \sum_{k=1}^{n} R_k + \lambda_1 (2A_1 + A_2 X^k (X_- + X_+) + A_3 X^{-k} (X_- + X_+)) + 2\lambda_2 R_k
\]

\[
= 2 \sum_{k=1}^{n} R_k + 2(\lambda_1 + \lambda_2) A_1 - 2\lambda_2 (A_2 X^k + A_3 X^{-k}) + 2\lambda_2 (A_2 X^k + A_3 X^{-k})
\]

\[
= 2 \sum_{k=1}^{n} R_k + 2(\lambda_1 + \lambda_2) A_1. \tag{80}
\]

Additionally, because of Eq. (64), we have

\[
\sum_{k=1}^{n} R_k = n A_1. \tag{81}
\]

In the meantime we can just sum up \( R_k \) to get \( \sum_{k=1}^{n} R_k \) as

\[
\sum_{k=1}^{n} R_k = n A_1 = \sum_{k=1}^{n} (A_1 + A_2 X^k + A_3 X^{-k}). \tag{82}
\]

Therefore,

\[
\sum_{k=1}^{n} (A_2 X^k + A_3 X^{-k}) = 0, \tag{83}
\]

\[
A_2 \frac{X(1 - X^n)}{1 - X} + A_3 \frac{X^{-1}(1 - X^{-n})}{1 - X^{-1}} = 0, \tag{84}
\]

\[
A_3 = A_2 \frac{X - X^{n+1}}{1 - X^{-n}} = -A_2 X^{n+1}. \tag{85}
\]

On the other hand, we have

\[
\sum_{k=1}^{n} R_k R_{k+1} = \sum_{k=1}^{n-1} R_k R_{k+1} + R_n R_1 = A_2^2 L_1(X) + A_1^2 n = b, \tag{86}
\]
where
\[
L_1(X) = \frac{(-X^2 + 2X + 1) X^{2n} + (-nX^4 + n + X^4 + 2X^3 - 2X - 1) X^n - X^4 - 2X^3 + X^2}{X^2 - 1}.
\] (87)

Therefore,
\[
A^2 = \frac{b - A^2 n}{L_1(X)}.
\] (88)

Plug \(A^2\) in the the summation of \(R_k^2\)
\[
\sum_{k=1}^{n} R_k^2 = A^2 n - \frac{2A^2 X (-X^{2n} + X^2 - 1) X^n + X)}{X^2 - 1} = 1,
\] (89)
then we have
\[
A^2 n - \frac{2(b - A^2 n) X (-X^{2n+1} + n (X^2 - 1) X^n + X)}{L_1(X)(X^2 - 1)} = 1.
\] (90)

Also, notice that \(O = (\sum_{k=1}^{n} R_k)^2 = n^2 A^2\) and Eq. (74). We have
\[
n^2 A^2 = \frac{2nX}{(X - 1)^2} (1 - b) + n.
\] (91)

Combine Eq. (90) and Eq. (91), we have
\[
0 = -\frac{2bnX}{(X - 1)^2} + \frac{2nX}{(X - 1)^2} + n - n^2 A^2
\]
\[
= \frac{2(b - 1) nX (X + 1)^2 (X - X^n) (X^n - 1)}{(X - 1)^2 ((3X + 1)X^{2n} + (X + 1) (n(X - 1)^2 - (X + 1)^2) X^n + (X + 3)X^2)}.
\] (92)

A necessary condition for the above equation is
\[
2(1 - b) nX^2 (X + 1)^2 (X^{n-1} - 1) (X^n - 1) = 0,
\] (93)
or equivalently,
\[
X = 0, X = -1, X = e^{i \frac{m}{n} 2\pi}, X = e^{i \frac{m}{n - 1} 2\pi}.
\] (94)

We needs to find out which solution of \(X\) to adopt. Define \(t\) as \(X = e^{i t}\). Then we have
\[
\frac{2X}{(X - 1)^2} = \frac{2e^{it}}{(-1 + e^{it})^2} = \frac{1}{\cos(t) - 1}
\] (95)
and
\[
O = \frac{n}{1 - \cos(t)} (b - 1) + n.
\] (96)

Obviously \(X \neq 0\) because \(X \neq -1, t \neq \pi\). \(O(b)\) is maximized when \(1 - \cos(t)\) is maximized and \(t\) mod \(2\pi\) should be as closed to \(\pi\) as possible. Here, we assume \(n > 3\) first. For the case \(n = 3\) it is trivial to see the result is the same. If \(X = e^{i \frac{m}{n+1} 2\pi}\), \(O\) is maximized when \(t = \pi \pm \frac{2\pi}{n+1}\). If \(X = e^{i \frac{m}{n} 2\pi}\), \(O\) is maximized when \(t = \pi \pm \frac{\pi}{n}\), which is closer to \(\pi\) than \(t = \pi \pm \frac{2\pi}{n+1}\). Therefore \(O\) is maximized when
\[
t = \pi \pm \frac{\pi}{n} = \frac{n + 1}{n} \pi.
\] (97)

Therefore,
\[
O(b) = \frac{n}{1 - \cos\left(\frac{n + 1}{n} \pi\right)} (b - 1) + n = \frac{n}{1 - \cos\left(\frac{n}{2} \pi\right)} (b - 1) + n.
\] (98)
Finally, we must deal with the condition when $X_+ = X_- = X = -1$. We will prove $X \neq -1$. Notice that, in this case, when $b = -1$, by Eq. (74), $O$ must be zero.

\[ R_k = A_1 + (A_2 + A_3 k)(-1)^k. \]  
(99)

Because $O = 0$,

\[ \sum_{k=1}^{n} R_k = \frac{1}{2} (2A_1 n - A_3 n - 2A_2 - A_3) = 0, \]
(100)

\[ A_1 = \frac{A_3 n + 2A_2 + A_3}{2n}. \]
(101)

Calculate $\sum_{k=1}^{n} R_k^2$ and $\sum_{k=1}^{n} R_k R_{k+1}$ and substitute $A_1$ by above equation, we have

\[ \sum_{k=1}^{n} R_k^2 = 1 = A_1^2 n + A_2^2 n + \frac{1}{6} A_3^2 n(n+1)(2n+1) + A_3(n+1)(A_2 n - A_1) - 2A_2 A_1 \]
\[ = \frac{1}{12n} (n^2 - 1) \left( A_3^2 (4n^2 + 6n + 3) + 12A_3 A_2 (n+1) + 12A_2^2 \right), \]
(102)

\[ \sum_{k=1}^{n} R_k R_{k+1} = -1 = A_1^2 n - A_1(A_3(n+1) + 2A_2) - \frac{1}{3} (n-2) \left( 3A_3 A_2 (n+1) + A_3^2 n(n+2) + 3A_2^2 \right) \]
\[ = - \frac{1}{12n} (n-1) \left( 12A_3 A_2 (n^2 - 1) + 12A_2^2 (n-1) + A_3^2 (n(4n+1) - 9) - 3 \right). \]
(103)

By the above two equations we can get

\[ \frac{(n-1) \left( A_3^2(-(n+3))(n+1) - 6 \right)}{6(n+1)} = -1, \]
(104)

which has no solution when $n = 3$. Thus, $X \neq -1$ when $n = 3$. Assume $n > 3$, we have

\[ A_3^2 = \frac{12}{(n-3)(n-1)(n+1)}. \]
(105)

Viewing Eq. (102) as a quadratic equation for $A_2$, the discriminant is

\[ \Delta = \frac{48n(12 + A_3^2(n^3))}{n^2 - 1} = \frac{1728n}{(3-n)(n^2-1)}. \]
(106)

Therefore, for $n > 3$, $A_2$ does not have real solution. Thus, we proved that $X \neq -1$ for every odd $n$ ($n > 1$).

In conclusion, for both even and odd $n$:

\[ O = \frac{n}{1 - \cos(\left\lfloor \frac{n}{2} \right\rfloor \frac{\pi}{n}} (b - 1) + n. \]
(107)

\[ \square \]

**Corollary 3.** Let $R$ be a vector of $n$ real numbers. Under the condition that $\sum_{i=1}^{n} R_i^2 = l (l \in (0, 1])$ and $\sum_{i=1}^{n} R_i R_{i+1} = b$ ($R_{n+1}$ is defined to be $R_1$), the maximum of $O = (\sum_{i=1}^{n} R_i)^2$ is

\[ O = \frac{n}{1 - \cos(\left\lfloor \frac{n}{2} \right\rfloor \frac{\pi}{n}} (b - l) + nl. \]
Proof. Assume the \( R \) that maximized \( O \) under the condition that \( \sum_{i=1}^{n} R_i^2 = l \) and \( \sum_{i=1}^{n} R_i R_{i+1} = b \). Then the vector \( T = \frac{R}{\sqrt{l}} \) satisfies the condition that \( \sum_{i=1}^{n} T_i^2 = 1 \) and \( \sum_{i=1}^{n} T_i T_{i+1} = \frac{b}{l} \). By Prop. (3) we know that

\[
(\sum_{i=1}^{n} T_i)^2 = \frac{1}{l} (\sum_{i=1}^{n} R_i)^2 \leq \frac{n}{1 - \cos\left(\frac{\pi}{n}\right)} \left(\frac{b}{l} - 1\right) + n. \tag{108}
\]

If the theorem we want to prove is not true and

\[
(\sum_{i=1}^{n} R_i)^2 > \frac{n}{1 - \cos\left(\frac{\pi}{n}\right)} (b - l) + nl, \tag{109}
\]

then

\[
(\sum_{i=1}^{n} T_i)^2 = \frac{1}{l} (\sum_{i=1}^{n} R_i)^2 > \frac{n}{1 - \cos\left(\frac{\pi}{n}\right)} \left(\frac{b}{l} - 1\right) + n. \tag{110}
\]

Eq. (108) and Eq. (110) are contradictory and then we prove the theorem.

\[\Box\]

**Theorem 3 (Babai [21]).** For any group oracle \( B \) there exists a randomized process \( P \) acting as follows. On input \( g_1, \ldots, g_k \in G(B_n) \) and \( \epsilon > 0 \), \( P \) outputs an element of \( H = \langle g_1, \ldots, g_k \rangle \) in time polynomial in \( n + \log 1/\epsilon \) such that each \( g \in H \) is output with probability in the range \( (1/|H| - \epsilon, 1/|H| + \epsilon) \).

**More experimental results**

For the input state \( \frac{1}{\sqrt{2}} (|B\rangle + |AB\rangle) = \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle) \), we present the detailed experimental imaginary matrix of the outputs here, as shown in Fig. 5.
FIG. 4. (Color online). Real parts of density matrices of the finial output photons for the case with input state of $(|HH⟩ + |VV⟩)/\sqrt{2}$. a-c represent the cases of initial state, output photons of $a$ and $b$ in E-type interferometer, output photons of $a$ and $b$ in AB-type interferometer without CNOT gate, respectively. e-g represent the cases of output photons of $a$ and $b$ in A-type interferometer (with fidelity 92.6 ± 2.4%), $a$ and $b$ in B-type interferometer (88.9 ± 0.7%), $a$ and $b$ in AB-type interferometer (88.5 ± 1.2%), respectively. i-k represent the cases of output photons of $a$ and $b$ in A-type interferometer (98.0 ± 0.3%), $a$ and $b$ in B-type interferometer (94.4 ± 0.3%), $a$ and $b$ in AB-type interferometer (94.8 ± 0.9%), respectively. d, h and l represent the corresponding theoretical predictions.
FIG. 5. (Color online). Imaginary parts of density matrices of the finial output photons for the case with input state of $\frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. a-c represent the cases of initial state, output photons of $a$ and $b$ in E-type interferometer, output photons of $a$ and $b$ in AB-type interferometer without CNOT gate, respectively. e-g represent the cases of output photons of $a$ and $b$ in A-type interferometer, $a$ and $b$ in B-type interferometer, $a$ and $b$ in AB-type interferometer, respectively. i-k represent the cases of output photons of $a$ and $b$ in A-type interferometer, $a$ and $b$ in B-type interferometer, $a$ and $b$ in AB-type interferometer, respectively. d, h and l represent the corresponding theoretical predictions.