cryptography

MDPI

Article

A Simple Protocol for Certifying Graph States and Applications in Quantum Networks

Damian Markham [1,*] and Alexandra Krause [1,2]

[1] Laboratoire d'Informatique de Paris 6, Centre National de la Recherche Scientifique (CNRS), Université Pierre et Marie Curie (UPMC)-Sorbonne Universites, 75005 Paris, France; alexandra.krause2@gmail.com

[2] Department of Physics, Freie Universität Berlin, 14194 Berlin, Germany

* Correspondence: damian.markham@lip6.fr

Received: 13 December 2019; Accepted: 17 January 2020; Published: 22 January 2020

check for updates

Abstract: We present a simple protocol for certifying graph states in quantum networks using stabiliser measurements. The certification statements can easily be applied to different protocols using graph states. We see, for example, how it can be used for measurement based verified quantum computation, certified sampling of random unitaries, quantum metrology and sharing quantum secrets over untrusted channels.

Keywords: verification; graph states; quantum information networks

1. Introduction

Graph states are a family of multipartite quantum states, defined in one to one correspondence with a simple graph [1]. They are incredibly useful resources across quantum information, acting as the key entanglement resource for error correction [2], measurement based quantum computation [3], quantum secret sharing [4] and more [1]. Furthermore, they can be implemented in many different ways, for example in optics [5–9] including on chip [10], in ion traps [11,12], super conducting qubits [13] and NV centres [14].

Many methods exist for testing graph states varying in the trust that must be assumed and the kind of statements that are made. With respect to trust assumptions, on the one hand techniques such as tomography [15] and entanglement witnesses [16] make assumptions about the source and measurements (essentially that they are honest but noisy). On the other hand tests which require the least trust, where neither the source nor the measurement devices are trusted, such as self testing [17], are incredibly demanding to implement in a way that closes all loopholes (necessary for security).

In this work we explore the mid ground, where (local) measurement devices are trusted, but sources and channels are not [7,18–21]. Our statements of confidence are tailored to this end, following the language of quantum authentication [22], particularly suited to applications for quantum networks. At the end of the protocol one gets a quantum output—the state we want to use—and a classical output—which tells us weather we accept or reject. A successful test for us is then one that always accepts an ideal source and outputs the ideal source state (completeness) and, if it accepts, the state is not too far from the ideal state (soundness—see below for technical definitions). With this in hand, we see how it can be used for certification for various quantum network tasks, in particular for delegated computation, generation of randomness, quantum metrology and quantum secret sharing.

For a given graph G with vertices V, and denoting $N(i)$ as the neighbours of $i \in V$, associating a qubit to each vertex, a graph state $|G\rangle$ on $|V| = n$ qubits is defined through the associated stabiliser equations

$$|G\rangle = S_i|G\rangle, \tag{1}$$

Cryptography **2020**, 4, 3; doi:10.3390/cryptography4010003 www.mdpi.com/journal/cryptography

where S_i are the graph stabiliser operators, with generators $S_i := X_i \otimes_{j \in N(i)} Z_j$ associated to each of the N veritces, and X_i and Z_i are Pauli operators. We denote the full stabiliser group $S = \{S_i\} =< S_1, ..., S_n >$, which has 2^N elements. We say that the graph state $|G\rangle$ is shared amongst n players, who, depending on the application may be in one physical location or distributed across a network.

The idea of the protocol is very straightforward. The players ask the source for M copies of the graph state. They choose at random one of these to be used, and all the rest are tested by randomly choosing a stabiliser operator and checking it returns the value $+1$. Since the malicious parties (the source, channel... everything except the players) do not know which copy will be tested or used beforehand, the only way they will always pass all the tests is if the players receive the intended graph state each all M times.

We begin in the next section by introducing the basic protocol, along with an example. We then provide the rigorous security statements, followed by several applications. We conclude with discussions on variants of the protocol, some possible further applications and comments on the scaling of the security parameter.

2. Protocol

Many variants of the protocol are possible, in ways that may depend on the application or implementation at hand. For clarity we present one particular simple variant of a protocol. After we will comment on other possibilities. We start in the standard assumption that the honest parties, the players, share a secret classical key $k = \{r, t\}$, composed of $r \in [1...M]$, $t = \{t_i\}_{i \neq r}$, $t_i \in [1, ..., 2^n]$ denoting $\mathcal{K}$ the set of all keys ($k \in \mathcal{K}$). The protocol follows the steps below.

1. The source distributes M n-partite systems to the n players. In the honest case, this will be M copies of the graph state $|G\rangle$.
2. For copy $i \neq r$, each player performs their part of the measurement of stabiliser S_{t_i}. If all the stabilisers output value $+1$, Accept, otherwise Reject.
3. For copy r the state is the quantum output of the protocol.

The variable M plays the role of security parameter (see (9)). We briefly comment on some variants. Different parts of the protocol can be changed depending on the application. Indeed even the way the secret keys are shared even before the first step may vary, as we will see for the application to secret sharing. The way that the outcomes of the test in step 2 is shared and acceptance or rejection decided may be important for different cases, for example if some players in the network are dishonest or not trusted. One may also want to lower the accept threshold in step 2 to allow for noisy resource states, for example accepting if something less than 100% of stabiliser tests give the correct output $+1$. We will come back to these variants at different points later, but for now we continue with the simplest version presented above.

We briefly present a small example to illustrate how the protocol works. In Figure 1 we illustrate the square graph associated to the graph state $|C4\rangle$. The generators of the stabiliser group are given by

$$\begin{aligned} S_1 &= X_1 \otimes Z_2 \otimes Z_3 \otimes I_4, \\ S_2 &= Z_1 \otimes X_2 \otimes I_3 \otimes Z_4, \\ S_3 &= Z_1 \otimes I_2 \otimes X_3 \otimes Z_4, \\ S_4 &= I_1 \otimes Z_2 \otimes Z_2 \otimes X_4. \end{aligned}$$

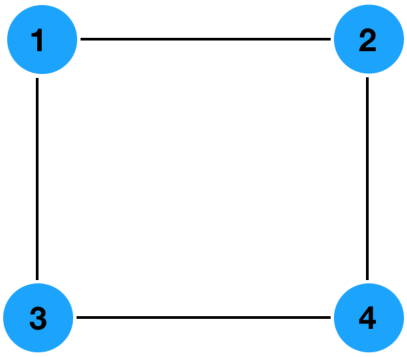

Figure 1. Example of a square graph state with four vertices $|C4\rangle$.

The stabiliser group $S =< S_1, S_2, S_3, S_4 >$ is the set of all products of the generators. In step 1 of the protocol the source is requested to generate M copies of the state $|C4\rangle$. In step two all but one of the copies (identified by r) are tested by each time randomly choosing one of the stabilisers to measure. For example if S_1 were chosen to be tested on the $i \neq r$th copy, the first party would measure X and parties two and three would measure Z. They would then compare all their answers, and if the product of their results was $+1$ they would accept. The example state here is the one of the simplest graph states, yet has been experimentally already used to demonstrate computation [23], error correction [24] and secret sharing [7]. The additional difficulty in performing our protocol to verify these applications is minimal as it just requires asking for many copies of the resource state, which is in any case how the set up works in all these implementations.

3. Security

We first formalise our notions of security, following [22]. For simplicity we encode the classical output as orthogonal quantum states $|ACC\rangle_R$ for accept and $|REJ\rangle_R$ for reject. The output state will in general depend on the classical key $k = \{r, t\}$. For each key $k \in \mathcal{K}$, we denote the output state of the players plus classical reference system as ρ^k. We say the protocol is ϵ-secure if it satisfies the following two properties

- **Completeness**. If the players recieve M copies of the ideal resource state $|G\rangle$, then for all keys k

$$\rho^k = |G\rangle_P\langle G| \otimes |ACC\rangle_R\langle ACC|. \tag{2}$$

- **Soundness**. Denoting the expected output state over all key strings as $\rho_{out} := \frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}} \rho^k$, and denoting the projection $P_{fail} := (I - |G\rangle_P\langle G|) \otimes |ACC\rangle_R\langle ACC|$, then

$$\text{Tr}\left(P_{fail}\rho_{out}\right) \leq \epsilon. \tag{3}$$

Completeness is trivially guaranteed since the test uses the stabilisers of the state itself, so it will always accept. Note that this definition of correctness is somewhat impractical, as one can never expect to have a perfect entangled state in any realistic source. However it is important in the sense of an ideal property of a protocol. Furthermore, our protocol can easily be adapted for more practical versions of completeness, as we discuss in the conclusions (see also Reference [25]).

Soundness follows through a similar reasoning to that in Reference [21]. Let us denote by ρ the state of all the Mn systems that the players receive in step 1 of the protocol. In order to bound (3) we only need to consider the output state conditioned on accept, let us denote it by ρ_{ACC}. To find this we start with the fact that for a given key $k = \{r, t\}$, the projection corresponding to accepting all $M - 1$ tests can be written as :

$$M^{r,t}_{accept} = \bigotimes_{i\neq r} \frac{(S_{t_i} + \mathbb{I}_i)}{2} \otimes \mathbb{I}_r. \tag{4}$$

From this we have that ρ_{ACC} can be written as

$$\rho_{ACC} = \sum_{r=1}^{M} \sum_{t} \frac{1}{M} \frac{1}{|S|^{M-1}} \rho_{r,t}, \tag{5}$$

with

$$\rho_{r,t} = \frac{1}{\mathrm{Tr}(M_{accept}^{r,t}\rho)} \mathrm{Tr}_{r^c}(M_{accept}^{r,t}\rho), \tag{6}$$

where A^c denotes the complement of set A.

Putting this together, we obtain

$$\mathrm{Tr}\left(P_{fail}\rho_{out}\right) = \frac{1}{M}\mathrm{Tr}\left(Q\rho\right), \tag{7}$$

where

$$\begin{aligned} Q &= \sum_{r=1}^{M} \sum_{t} \frac{1}{S^{M-1}} \bigotimes_{i \neq r} \frac{S_{t_i} + \mathbb{I}_i}{2} \otimes (\mathbb{I}_r - |G\rangle\langle G|) \\ &= \sum_{r=1}^{M} \bigotimes_{i \neq r} \frac{\mathbb{I}_i + |G\rangle_i \langle G|}{2} \otimes (\mathbb{I}_r - |G\rangle_r \langle G|), \end{aligned} \tag{8}$$

since $1/|S| \sum_i S_i = |G\rangle\langle G|$. Note that Q is hermitian and positive. It then remains to check that all eigenvalues of Q are smaller than 1, for which a proof can be found in the Appendix A. It then follows that

$$\mathrm{Tr}(P_{fail}\rho_{out}) \leq \frac{1}{M}, \tag{9}$$

for all source states ρ.

The protocol also has natural extensions for higher prime dimensional graph states, where proofs also follow straightforwardly.

Below we present several applications, where the security follows directly as above with a simple application of our protocol, or slight variants of the security statement are made (verified t-designs) or some of the variants of the simplest protocol mentioned above give the utility required (quantum secret sharing).

4. Applications

We focus on applications that can be considered as completely positive trace preserving (CPTP) map Γ acting on the quantum output. Since fidelity is monotonic under CPTP maps, the usefulness or soundness is preserved. This is the case, for example, when further interaction with the source is not required to run the protocol.

Formally, with respect to the CPTP application Γ one defines a new fail projector,

$$P_{Fail}(\Gamma) := (I - \Gamma(|G\rangle\langle G|)) \otimes |ACC\rangle\langle ACC|. \tag{10}$$

Due to the monotonicity of fidelity, (3) implies that

$$Tr\left(P_{fail}^{\Gamma(G)}\Gamma(\rho_B)\right) \leq \frac{1}{M}. \tag{11}$$

We now go through some examples of applications.

4.1. Verified Blind Quantum Computation

In verified blind quantum computation a technologically limited Alice wishes to delegate some quantum computational task to a server, Bob, in such a way that Bob does not get information about the computation (blind), and moreover, that she can be confident the computation has been carried out correctly (verified). There are many techniques to achieve this—see Reference [26] for a recent overview.

In our scenario Alice is limited to single qubit measurements. Clearly this, on its own, is not enough for universal quantum computation. However, in measurement based quantum computation (MBQC), universal quantum computation is achieved by single qubit measurements on a graph state, with feed forward [3]. Importantly the measurements can be made one qubit at a time. Thus, if Alice asks Bob to provide her with a universal graph states, either cluster states [3] or brickwork states [27] for example—Alice can perform the computation she wants. Moreover this is blind to Bob—he gets only minimal information, an upper bound to the size of the computation (given by the size of the graph state Alice asks for). To verify the computation Alice can simply apply our protocol to test and use a universal graph state of her choice.

One has the same notions of completeness and soundness as those above, replacing the graph state by the ideal output of the computation. Completeness follows immediately from the universality of the chosen graph state. For soundness, we simply note that Alice's measurement sequence, which affects the computation, can be understood entirely as a CPTP map on the quantum output of our protocol. In this way, the condition (11) ensures soundness also. More specifically, if we denote the ideal output of a computation as ρ_{ideal}^{comp}, and the average output of a given computation ρ_{out}^{comp}, the failing projector becomes $P_{Fail}^{comp} := \left(I - \rho_{ideal}^{comp}\right) \otimes |ACC\rangle\langle ACC|$, and we have from (11) a verification soundness condition (see e.g., Reference [28]),

$$Tr\left(P_{Fail}^{comp}\rho_{out}^{comp}\right) \leq \frac{1}{M}. \tag{12}$$

Note that, compared to Reference [28], this scaling with resources is poor. We will talk about this in the conclusions, but it is essentially a trade-off between the security scaling, and the entanglement costs of the protocol. In this sense our protocol sacrifices scaling for practicability.

We also note that the idea of testing graph states for MBQC computation has been presented before in several measurement based verification schemes, for example, References [29,30]. Indeed, this application of our protocol is almost identical to the verified computation scheme in Reference [30], the main differences being in the specifics of the test (we measure settings chosen from all stabilisers, they a subset) and the figure of merit used (we use the correctness and soundess above, they use the language of hypothesis testing). We present it here simply as an alternative possible scheme, with similar characteristics. As pointed out in Reference [30], this scenario is suited to performing fault tolerant computation, since Alice could equally ask Bob for a resource graph state for fault tolerant computation, for example the topological scheme in Reference [31] using 3D cluster states. This was the idea of the fault tolerant verified computation presented in Reference [32], note however that this works only if the errors on Alice's measurement device are assumed to be independent from anything happening on Bob's side.

4.2. Verified t-Designs

Graph states can also be used to sample from a random ensemble of unitaries—this is effectively MBQC without correction, where the measurement outcomes index which unitary is implemented. In particular, in Reference [33] it was shown that ensembles with a particularly useful property of being t-designs can be efficiently sampled using graph states. A t-design is an ensemble of unitaries with the property that its statistical moments match those of a Haar ensemble up to order t, with applications across quantum information and physics, for example in estimating noise [34], private channels [35], modelling thermalisation [36], photonics [37], and even black hole physics [38]. Later in

Reference [39] this approach was developed to show that efficient t-designs can be generated using a regular lattice similar to the brickwork state. Both results rely heavily on the construction of [40,41] using random circuits.

Our protocol can be used to certify the application of a t-design random unitary onto an input, where the source of the graph state is not trusted. For each set of measurement outcomes $\bar{m}$, we denote the applied CPTP map on the graph state as $\Gamma^{\bar{m}}$. For simplicity we consider the action of the induced unitary on the input vertices $I \subset V$ corresponing to inputs in the state $|+\rangle$. Then [33,39] state that measurement result $\bar{m}$, occuring with probability $p_{\bar{m}}$ applies a unitary on the input $|+\rangle^{\otimes |I|}$

$$\Gamma^{\bar{m}}(|G\rangle) = U^{\bar{m}}|+\rangle^{\otimes |I|}, \tag{13}$$

such that the ensemble $\{p_{\bar{m}}, U^{\bar{m}}\}$ is an approximate t-design (see Reference [33] for detailed definitions).

For security of verified t-designs one can replace the graph state in the definitions (2) and (3) by the output state (13). The soundness is then guaranteed for each $\bar{m}$ by (11). It can easily be seen that one can flip this around to give a statement on the fidelity,

$$F(U^{\bar{m}}|\psi\rangle, \Gamma^{\bar{m}}(\rho_{ACC}))^2 \geq 1 - \frac{1}{P_{acc}M}, \tag{14}$$

where P_{acc} is the probability of passing the tests and ρ_{ACC} is the output of the protocol conditioned on accepting.

4.3. Quantum Metrology

In quantum metrology entangled states are used to measure with more precision than is possible with classical probes [42]. The general setting can be understood as an interferometer which imparts a phase ψ on one arm, each time a system passes through it. The idea is to send in many probes N in an entangled state ρ, whereafter measurements can reveal the phase with higher precision than possible sending in separable states.

How well this process allows the parameter ψ to be estimated is quantified by the *Quantum Fisher Information*, $\mathcal{F}_Q(\rho)$. Note, as indicated by the notation, for a simple interferometer the quantum Fisher information is independent of the value of ψ since it is unitarily encoded [43,44]. In particular, for ν independent repetitions of the process, the precision is characterised by the mean squared error $\Delta^2\tilde{\psi}$ of a (consistent and unbiased) estimator $\tilde{\psi}$, which is lower bounded by the *Quantum Cramér-Rao Bound* [45],

$$\Delta^2\tilde{\psi} \geq \frac{1}{\nu \mathcal{F}_Q(\rho)}. \tag{15}$$

For the standard interferometer, the best possible scaling with N is achieved by the N-party GHZ state $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$. Denoting its density matrix ρ_{GHZ} we have $\mathcal{F}_Q(\rho_{GHZ}) = N^2$. The GHZ state is locally equivalent to a graph state for the fully connected graph. Our certification protocol can easily be adapted using the same local unitaries to test ρ_{GHZ} (simply by rotating the test measurements accordingly).

In Reference [44], they show that the quantum Fisher information of two states differs by an amount bounded by their fidelity

$$\left|\mathcal{F}_Q(\rho) - \mathcal{F}_Q(\sigma)\right| \leq 6\sqrt{1 - F(\rho,\sigma)^2}N^2, \tag{16}$$

if ρ or σ are pure. That is, if two states are close, as measured by their fidelity, their usefulness for quantum metrology is close. Given the fidelity bound implied by our test (14), we see that the quantum

Fisher information is also bounded. For the rotated protocol testing a GHZ states, given the output state conditioned on accepting ρ_{ACC}, we have,

$$\mathcal{F}_Q(\rho_{ACC}) \geq N^2 \left(1 - \frac{6}{P_{ACC}M}\right). \tag{17}$$

4.4. Secret Sharing over Untrusted Channels

In quantum secret sharing a dealer wishes to distribute a secret quantum state amongst N players such that only certain subsets of players can access the secret—the authorised sets. It was shown in References [4,46] that any secret sharing scheme can be implemented using graph states. However, these rely on the trusted sharing of the graph state. If we are careful, a variant of our protocol can be used to boost these protocols to one where the network of dealer and players do not need to trust the source of the graph state or the channels used to share them.

There are two important subtleties in the application of our protocol here, stemming from the fact that unauthorised sets of players should be treated as adversaries. Firstly, it makes their inclusion in the stabiliser tests not ideal. Secondly, if they also have access to the random key k this could potentially allow attacks. In Reference [21] a protocol was presented which can be understood as a variant of the application of our scheme where (i) the stabiliser tests are restricted to an authorised set, and (ii) the classical key k is distributed by a classical secret sharing scheme, with the same access structure. A proof of principle example of this protocol was implemented in Reference [7], demonstrating its simplicity.

5. Conclusions

In this work we have presented a protocol for certifying graph states and a few applications in quantum networks. There are clearly some applications that our protocol would not be suited for—namely ones where further interactions are required with Bob. Such interactions may allow for Bob to correlate his strategy in cheating the 'test' part to the future applications potentially threatening functionality (be it security or otherwise). Nevertheless its simplicity lends itself to many applications as we have seen, not only in the form of protocol presented here, but also its suitability to permit variants, as with secret sharing. A simple variant can also deal with noisy states for example, where one would not expect, even an honest noisy source to pass all the time. In such a case one can change the accept requirement to require some smaller portion of correct answers. One can adapt the security statements and proofs to this end without too much difficulty. Indeed, this is the approach taken in follow up work [25].

We also note that the fidelity of a state to particular graph states can be used as a witness for genuine multipartite entanglement (that is, entanglement which cannot be considered as entanglement between fewer than all the systems) [47]. In this way our protocol can be used to demonstrate this feature also. A related notion is genuine multipartite steering [48], where one considers the capacity of a state to violate a steering inequality [49] across all bipartitions. The fidelity to certain graph states is also known be usable as a witness for genuine multipartite steering [50]. In both these cases, the standard approach uses stabiliser measurements, but assumes that the source is preparing identical copies of the state in each round [47,48,50]. Our protocol relaxes this assumption, yet still allows for witnessing these features within confidence levels.

We end with a discussion on scaling of soundness condition with M. In the kind of protocol presented here, it is impossible to beat the $1/M$ scaling. This is clear simply because a malicious party can behave honestly for all but one requested state, and send one false/dishonest state. With probability $1/M$ the malicious party's choice of when to be dishonest coincides with the users choice of which one would be used and not tested, so strategy passes the test perfectly yet the state can be arbitrarily far from the ideal one and potentially ruin whatever application. Thus in order to beat the $1/M$ scaling one expects to need some more entanglement. This can be done, for example, by encoding the desired state on some randomly chosen error correcting code—the essential trick used in the original authentication paper by Barnum et al. [22]. Such an approach can give an exponential scaling in security with the number of systems sent. The downside now is that the entanglement required scales with the security. This then suggests a tradeoff between entanglement and scaling.

In this context, the advantage of our protocol is that, for many applications, the difficulty in implementing a certified version of an application becomes only the same difficulty as producing the same resource state many times, rather than asking for much more difficult larger, scaling, entanglement. In optics for example, this advantage makes certified secret sharing possible [7], doing so an entangled code version would require impractical scaling in entanglement.

Author Contributions: Conceptualization, D.M. and A.K.; Methodology, D.M. and A.K.; Writing—review & editing, D.M. and A.K. All authors have read and agreed to the published version of the manuscript.

Funding: AK is grateful to the ERASMUS program which supported the visit resulting in this collaboration. DM is grateful for funding from ANR COMB.

Acknowledgments: We thank Elham Kashefi, Peter Turner, Gérard Duchamp, Tomoyuki Morimae and Juani Bermejo Vega for useful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

We can write Q (8) as

$$Q = \sum_{r=1}^{M} Q_r \tag{A1}$$

with

$$Q_r = \bigotimes_{i \neq r} \frac{\mathbb{I}_i + |G\rangle_i \langle G|}{2} \otimes (\mathbb{I}_r - |G\rangle_r \langle G|) \tag{A2}$$

Define A as $\frac{\mathbb{I}+|G\rangle\langle G|}{2}$ and B as $\mathbb{I} - |G\rangle\langle G|$.

An eigenvector for A with eigenvalue 1 is just given by $|G\rangle$. Denoting $|G'\rangle$ an eigenvector with eigenvalue 1 of B, an complete eigenbasis for Q is given by all possible combinations of tensor products of those vectors. B acts on $|G\rangle$ as $B|G\rangle = |G\rangle - |G\rangle = 0$ while $A|G'\rangle = \frac{|G'\rangle}{2} + \frac{|G\rangle\langle G|G'\rangle}{2} = \frac{|G'\rangle}{2}$ as $\langle G|G'\rangle = 0$.

We can then write $Q_r = \bigotimes_{i=1}^{r-1} A_i \otimes B_r \bigotimes_{l=r+1}^{M} A_l$ where r denotes the position of B in the tensor. We then denote the k-th family of eigenvectors where $|G'\rangle$ appears k times as $|Eig\rangle_k = \bigotimes_{j \neq k} |G\rangle_k \bigotimes_{k \neq j} |G'\rangle_k | k + j = M$

Trying to determinate the action from Q_r on $|Eig\rangle_k$, we have to distinguish the following cases :

Let r be in $[1, M-k]$. $|G\rangle$ will then be projected to the eigenvalue 0 so that these cases are trivial. Regarding r in $[k, M]$ gives us $B|G'\rangle = |G'\rangle$. After then, A acts for $k-1$ times on $|G'\rangle$ giving the eigenvalue $\frac{1}{2^{k-1}}$.

Putting this together and regarding the symmetry of Q with respect to permutations of r within the sum the distribution of $|G\rangle$ and $|G'\rangle$ in the eigenvectors does not matter. It suffices to know, how often $|G'\rangle$ appears. The sum contains $M-k$ elements with eigenvalue 0 and the remaining k elements with eigenvalue $\frac{1}{2^{k-1}}$. The summation gives than as eigenvalue $\frac{k}{2^{k-1}}$ for every $|Eig\rangle_k$, which is always below one.

References

1. Hein, M.; Eisert, J.; Briegel, H.J. Multiparty entanglement in graph states. *Phys. Rev. A* **2004**, *69*, 062311. [CrossRef]
2. Schlingemann, D.; Werner, R.F. Quantum error-correcting codes associated with graphs. *Phys. Rev. A* **2001**, *65*, 012308. [CrossRef]
3. Raussendorf, R.; Briegel, H.J. A one-way quantum computer. *Phys. Rev. Lett.* **2001**, *86*, 5188. [CrossRef]

4. Markham, D.; Sanders, B.C. Graph states for quantum secret sharing. *Phys. Rev. A* **2008**, *78*, 042309. [CrossRef]
5. Wang, X.L.; Chen, L.K.; Li, W.; Huang, H.L.; Liu, C.; Chen, C.; Luo, Y.H.; Su, Z.E.; Wu, D.; Li, Z.D.; et al. Experimental ten-photon entanglement. *Phys. Rev. Lett.* **2016**, *117*, 210502. [CrossRef]
6. Barz, S.; Kashefi, E.; Broadbent, A.; Fitzsimons, J.F.; Zeilinger, A.; Walther, P. Demonstration of blind quantum computing. *Science* **2012**, *335*, 303–308. [CrossRef]
7. Bell, B.; Markham, D.; Herrera-Martí, D.; Marin, A.; Wadsworth, W.; Rarity, J.; Tame, M. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **2014**, *5*, 1–12. [CrossRef]
8. Cai, Y.; Roslund, J.; Ferrini, G.; Arzani, F.; Xu, X.; Fabre, C.; Treps, N. Multimode entanglement in reconfigurable graph states using optical frequency combs. *Nat. Commun.* **2017**, *8*, 15645. [CrossRef]
9. Yokoyama, S.; Ukai, R.; Armstrong, S.C.; Sornphiphatphong, C.; Kaji, T.; Suzuki, S.; Yoshikawa, J.I.; Yonezawa, H.; Menicucci, N.C.; Furusawa, A. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. *Nat. Photonics* **2013**, *7*, 982–986. [CrossRef]
10. Ciampini, M.A.; Orieux, A.; Paesani, S.; Sciarrino, F.; Corrielli, G.; Crespi, A.; Ramponi, R.; Osellame, R.; Mataloni, P. Path-polarization hyperentangled and cluster states of photons on a chip. *Light Sci. Appl.* **2016**, *5*, e16064. [CrossRef]
11. Barreiro, J.T.; Müller, M.; Schindler, P.; Nigg, D.; Monz, T.; Chwalla, M.; Hennrich, M.; Roos, C.F.; Zoller, P.; Blatt, R. An open-system quantum simulator with trapped ions. *Nature* **2011**, *470*, 486–491. [CrossRef] [PubMed]
12. Monz, T.; Schindler, P.; Barreiro, J.T.; Chwalla, M.; Nigg, D.; Coish, W.A.; Harlander, M.; Hänsel, W.; Hennrich, M.; Blatt, R. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.* **2011**, *106*, 130506. [CrossRef] [PubMed]
13. Song, C.; Xu, K.; Liu, W.; Yang, C.P.; Zheng, S.B.; Deng, H.; Xie, Q.; Huang, K.; Guo, Q.; Zhang, L.; et al. 10-qubit entanglement and parallel logic operations with a superconducting circuit. *Phys. Rev. Lett.* **2017**, *119*, 180511. [CrossRef] [PubMed]
14. Cramer, J.; Kalb, N.; Rol, M.A.; Hensen, B.; Blok, M.S.; Markham, M.; Twitchen, D.J.; Hanson, R.; Taminiau, T.H. Repeated quantum error correction on a continuously encoded qubit by real-time feedback. *Nat. Commun.* **2016**, *7*, 1–7. [CrossRef] [PubMed]
15. D'Ariano, G.M.; Paris, M.G.; Sacchi, M.F. Quantum tomography. *Adv. Imaging Electron Phys.* **2003**, *128*, 206–309.
16. Jungnitsch, B.; Moroder, T.; Gühne, O. Entanglement witnesses for graph states: General theory and examples. *Phys. Rev. A* **2011**, *84*, 032310. [CrossRef]
17. McKague, M. Self-testing graph states. In *Conference on Quantum Computation, Communication, and Cryptography*; Springer: Berlin, Germany, 2011; pp. 104–120.
18. Pappa, A.; Chailloux, A.; Wehner, S.; Diamanti, E.; Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **2012**, *108*, 260502. [CrossRef]
19. Lyons, D.W.; Walck, S.N. Entanglement verification using local unitary stabilizers. *Phys. Rev. A* **2013**, *87*, 062321. [CrossRef]
20. McCutcheon, W.; Pappa, A.; Bell, B.; McMillan, A.; Chailloux, A.; Lawson, T.; Mafu, M.; Markham, D.; Diamanti, E.; Kerenidis, I.; et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **2016**, *7*, 13251. [CrossRef]
21. Markham, D.; Marin, A. Practical Sharing of Quantum Secrets over Untrusted Channels. In *International Conference on Information Theoretic Security*; Springer: Cham, Switzerland, 2015; pp. 1–14.
22. Barnum, H.; Crépeau, C.; Gottesman, D.; Smith, A.; Tapp, A. Authentication of quantum messages. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, BC, Canada, 19 November 2002; pp. 449–458.
23. Walther, P.; Resch, K.J.; Rudolph, T.; Schenck, E.; Weinfurter, H.; Vedral, V.; Aspelmeyer, M.; Zeilinger, A. Experimental one-way quantum computing. *Nature* **2005**, *434*, 169. [CrossRef]
24. Bell, B.; Herrera-Martí, D.; Tame, M.; Markham, D.; Wadsworth, W.; Rarity, J. Experimental demonstration of a graph state quantum error-correction code. *Nat. Commun.* **2014**, *5*, 1–10. [CrossRef] [PubMed]
25. Unnikrishnan, A.; Markham, D. Authenticated teleportation and verification in a noisy network. *arXiv* **2019**, arXiv:1911.07000.
26. Gheorghiu, A.; Kapourniotis, T.; Kashefi, E. Verification of quantum computation: An overview of existing approaches. *Theory Comput. Syst.* **2019**, *63*, 715–808. [CrossRef]

27. Broadbent, A.; Fitzsimons, J.; Kashefi, E. Universal blind quantum computation. In Proceedings of the FOCS'09—50th Annual IEEE Symposium on Foundations of Computer Science, 2009, Atlanta, GA, USA, 25–27 October 2009; pp. 517–526.
28. Fitzsimons, J.F.; Kashefi, E. Unconditionally verifiable blind computation. *arXiv* **2012**, arXiv:1203.5217.
29. Hayashi, M.; Hajdusek, M. Self-guaranteed measurement-based quantum computation. *arXiv* **2016**, arXiv:1603.02195.
30. Hayashi, M.; Morimae, T. Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.* **2015**, *115*, 220502. [CrossRef]
31. Raussendorf, R.; Harrington, J.; Goyal, K. Topological fault-tolerance in cluster state quantum computation. *New J. Phys.* **2007**, *9*, 199. [CrossRef]
32. Fujii, K.; Hayashi, M. Verifiable fault tolerance in measurement-based quantum computation. *Phys. Rev. A* **2017**, *96*, 030301. [CrossRef]
33. Turner, P.S.; Markham, D. Derandomizing quantum circuits with measurement-based unitary designs. *Phys. Rev. Lett.* **2016**, *116*, 200501. [CrossRef]
34. Emerson, J.; Weinstein, Y.S.; Saraceno, M.; Lloyd, S.; Cory, D.G. Pseudo-random unitary operators for quantum information processing. *Science* **2003**, *302*, 2098–2100. [CrossRef]
35. Hayden, P.; Leung, D.; Shor, P.W.; Winter, A. Randomizing quantum states: Constructions and applications. *Commun. Math. Phys.* **2004**, *250*, 371–391. [CrossRef]
36. Müller, M.P.; Adlam, E.; Masanes, L.; Wiebe, N. Thermalization and canonical typicality in translation-invariant quantum lattice systems. *Commun. Math. Phys.* **2015**, *340*, 499–561.
37. Matthews, J.C.; Whittaker, R.; O'Brien, J.L.; Turner, P.S. Testing randomness with photons by direct characterization of optical t-designs. *Phys. Rev. A* **2015**, *91*, 020301. [CrossRef]
38. Hayden, P.; Preskill, J. Black holes as mirrors: Quantum information in random subsystems. *J. High Energy Phys.* **2007**, *2007*, 120. [CrossRef]
39. Mezher, R.; Ghalbouni, J.; Dgheim, J.; Markham, D. Efficient quantum pseudorandomness with simple graph states. *Phys. Rev. A* **2018**, *97*, 022333. doi:10.1103/PhysRevA.97.022333. [CrossRef]
40. Brandão, F.G.; Harrow, A.W.; Horodecki, M. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.* **2016**, *346*, 397–434.
41. Brandão, F.G.; Harrow, A.W.; Horodecki, M. Efficient Quantum Pseudorandomness. *Phys. Rev. Lett.* **2016**, *116*, 170502.
42. Giovannetti, V.; Lloyd, S.; Maccone, L. Advances in quantum metrology. *Nat. Photonics* **2011**, *5*, 222–229. [CrossRef]
43. Tóth, G.; Apellaniz, I. Quantum metrology from a quantum information science perspective. *J. Phys. A Math. Theor.* **2014**, *47*, 424006.
44. Augusiak, R.; Kołodyński, J.; Streltsov, A.; Bera, M.N.; Acin, A.; Lewenstein, M. Asymptotic role of entanglement in quantum metrology. *Phys. Rev. A* **2016**, *94*, 012339. [CrossRef]
45. Braunstein, S.L.; Caves, C.M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.* **1994**, *72*, 3439. [CrossRef] [PubMed]
46. Keet, A.; Fortescue, B.; Markham, D.; Sanders, B.C. Quantum secret sharing with qudit graph states. *Phys. Rev. A* **2010**, *82*, 062315. [CrossRef]
47. Tóth, G.; Gühne, O. Detecting genuine multipartite entanglement with two local measurements. *Phys. Rev. Lett.* **2005**, *94*, 060501.
48. He, Q.; Reid, M. Genuine multipartite Einstein-Podolsky-Rosen steering. *Phys. Rev. Lett.* **2013**, *111*, 250403. [CrossRef]
49. Cavalcanti, E.G.; Hall, M.J.; Wiseman, H.M. Entanglement verification and steering when Alice and Bob cannot be trusted. *Phys. Rev. A* **2013**, *87*, 032306. [CrossRef]
50. Li, C.M.; Chen, K.; Chen, Y.N.; Zhang, Q.; Chen, Y.A.; Pan, J.W. Genuine high-order einstein-podolsky-rosen steering. *Phys. Rev. Lett.* **2015**, *115*, 010402. [CrossRef]