Pallister, S., Linden, N., & Montanaro, A. (2018). Optimal Verification of Entangled States with Local Measurements. *Physical Review Letters*, *120*(17), [170502]. https://doi.org/10.1103/PhysRevLett.120.170502

Optimal Verification of Entangled States with Local Measurements

Sam Pallister,[1,2,*] Noah Linden,[1,†] and Ashley Montanaro[1,‡]
[1]*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*
[2]*Quantum Engineering Centre for Doctoral Training, University of Bristol, Bristol BS8 1FD, United Kingdom*

(Received 18 September 2017; published 24 April 2018)

Consider the task of verifying that a given quantum device, designed to produce a particular entangled state, does indeed produce that state. One natural approach would be to characterize the output state by quantum state tomography, or alternatively, to perform some kind of Bell test, tailored to the state of interest. We show here that neither approach is optimal among local verification strategies for 2-qubit states. We find the optimal strategy in this case and show that quadratically fewer total measurements are needed to verify to within a given fidelity than in published results for quantum state tomography, Bell test, or fidelity estimation protocols. We also give efficient verification protocols for any stabilizer state. Additionally, we show that requiring that the strategy be constructed from local, nonadaptive, and noncollective measurements only incurs a constant-factor penalty over a strategy without these restrictions.

DOI: 10.1103/PhysRevLett.120.170502

Efficient and reliable quantum state preparation is a necessary step for all quantum technologies. However, characterization and verification of such devices is typically a time-consuming and computationally difficult process. For example, tomographic reconstruction of a state of eight ions required taking ~650 000 measurements over 10 h and a statistical analysis that took far longer [1]. Verification of a few-qubit photonic state is similarly challenging [2,3]. This is also the case in tomography of continuous-variable systems [4–6]. One may instead resort to nontomographic methods to verify that a device reliably outputs a particular state, but such methods typically either, (a) assume that the output state is within some special family of states, for example, in compressed sensing [7,8] or matrix product state tomography [9], or (b) extract only partial information about the state, such as when estimating entanglement witnesses [10,11].

Here, we derive the optimal local verification strategy for common entangled states and compare its performance to bounds for nonadaptive quantum state tomography in [12] and the fidelity estimation protocol in [13]. Specifically, we demonstrate nonadaptive verification strategies for arbitrary 2-qubit states and stabilizer states of N qubits that are constructed from local measurements and require quadratically fewer copies to verify to within a given fidelity than for these previous protocols. Moreover, the requirement that the measurements be local incurs only a constant-factor penalty over the best nonlocal strategy, even if collective and adaptive measurements are allowed.

Premise.—Colloquially, a quantum state verification protocol is a procedure for gaining confidence that the output of some device is a particular state over any other. However, for any scheme involving measurements on a finite number of copies of the output state, one can always find an alternative state within some sufficiently small distance that is guaranteed to fool the verifier. Furthermore, the outcomes of measurements are, in general, probabilistic and a verification protocol collects a finite amount of data, and so any statement about verification can only be made up to some finite statistical confidence. The only meaningful statement to make in this context is the statistical inference that the state output from a device sits within a ball of a certain small radius (given some metric) of the correct state, with some statistical confidence. Thus, the outcome of a state verification protocol is a statement like “the device outputs copies of a state that has 99% fidelity with the target, with 90% probability.” Note that this is different from the setting of state tomography; a verification protocol answers the question “Is the state $|\psi\rangle$?” rather than the more involved tomographic question “Which state do I have?” Hence, unlike tomography, a verification protocol may give no information about the true state if the protocol fails.

We now outline the framework for verification protocols that we consider. Take a verifier with access to some set of allowed measurements and a device that produces states $\sigma_1, \sigma_2, \ldots, \sigma_n$, which are supposed to all be $|\psi\rangle$, but may in practice be different from $|\psi\rangle$ or each other. We have the promise that either $\sigma_i = |\psi\rangle\langle\psi|$ for all i or $\langle\psi|\sigma_i|\psi\rangle \leq 1-\epsilon$ for all i. The verifier must determine which is the case with worst-case failure probability δ.

The protocol proceeds as follows. For each σ_i, the verifier randomly draws a binary-outcome projective measurement $\{P_j, \mathbb{1} - P_j\}$ from a prespecified set $\mathcal{S}$ with some probability μ_j^i. Label the outcomes "pass" and "fail"; in a pass instance, the verifier continues to state σ_{i+1}, otherwise the protocol ends and the verifier concludes that the state was not $|\psi\rangle$. If the protocol passes on all n states, then the verifier concludes that the state was $|\psi\rangle$. We impose the constraint that every $P_j \in \mathcal{S}$ *always* accepts when $\sigma_i = |\psi\rangle\langle\psi|$, $\forall i$ (i.e., that $|\psi\rangle$ is in the pass eigenspace of every projector $P_j \in \mathcal{S}$). This may seem a prohibitively strong constraint, but we later demonstrate that it is both achievable for the sets of states we consider and is always asymptotically favorable to the verifier.

The maximal probability that the verifier passes on copy i is

$$\mathrm{Prob}[\text{Pass on copy } i] = \max_{\substack{\sigma \\ \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon}} \mathrm{tr}(\Omega_i \sigma), \tag{1}$$

where $\Omega_i = \sum_j \mu_j^i P_j$. However, the verifier seeks to minimize this quantity for each Ω_i and hence it suffices to take a fixed set of probabilities and projectors $\{\mu_j, P_j\}$, independent of i. Then the verifier-adversary optimization is

$$\min_{\Omega} \max_{\substack{\sigma \\ \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon}} \mathrm{tr}(\Omega\sigma) \coloneqq 1 - \Delta_\epsilon, \tag{2}$$

where $\Omega = \sum_j \mu_j P_j$. We call Ω a "strategy." Δ_ϵ is the expected probability that the state σ fails a single measurement. Then the maximal worst-case probability that the verifier fails to detect that we are in the "bad" case that $\langle\psi|\sigma_i|\psi\rangle \leq 1 - \epsilon$ for all i is $(1 - \Delta_\epsilon)^n$, so to achieve confidence $1 - \delta$, it is sufficient to take

$$n \geq \frac{\ln \delta^{-1}}{\ln[(1 - \Delta_\epsilon)^{-1}]} \approx \frac{1}{\Delta_\epsilon} \ln \delta^{-1}. \tag{3}$$

Protocols of this form satisfy some useful operational properties: (i) Nonadaptivity: the strategy is fixed from the outset and depends only on the mathematical description of $|\psi\rangle$, rather than the choices of any prior measurements or their measurement outcomes. (ii) Future proofing: the strategy is independent of the infidelity ϵ and gives a viable strategy for any choice of ϵ. Thus, an experimentalist is able to arbitrarily decrease the infidelity ϵ within which verification succeeds by simply taking more total measurements following the strategy prescription, rather than modifying the prescription itself. The experimentalist is free to choose an arbitrary $\epsilon > 0$ and be guaranteed that the strategy still works in verifying $|\psi\rangle$.

One may consider more general nonadaptive verification protocols given $\mathcal{S}$ and $\{\sigma_i\}$, where measurements do not output pass with certainty given input $|\psi\rangle$, and the overall determination of whether to accept or reject is based on a more complicated estimator built from the relative frequency of pass and fail outcomes. However, we show in the Supplemental Material [14] that these strategies require, asymptotically, quadratically more measurements in ϵ than those where $|\psi\rangle$ is always accepted. We will also see that the protocol outlined above achieves the same scaling with ϵ and δ as the globally optimal strategy, up to a constant factor, and so any other strategy (even based on nonlocal, adaptive, or collective measurements) would yield only, at most, constant-factor improvements.

Given no constraints on the verifier's measurement prescription, the optimal strategy is to just project onto $|\psi\rangle$. In this case, the fewest number of measurements needed to verify to confidence $1 - \delta$ and fidelity $1 - \epsilon$ is $n_{\mathrm{opt}} = \{-1/[\ln(1-\epsilon)\} \ln(1/\delta) \approx (1/\epsilon)\ln(1/\delta)$ (see the Supplemental Material [14]). However, in general, the projector $|\psi\rangle\langle\psi|$ will be nonlocal, which has the disadvantage of being harder to implement experimentally. This is particularly problematic in quantum optics, for example, where deterministic, unambiguous discrimination of a complete set of Bell states is impossible [15–17]. Thus, for each copy, there is a fixed probability of the measurement returning a "null" outcome; hence, regardless of the optimality of the verification strategy, merely the probability of its successful operation decreases exponentially with the number of measurements. Instead, we seek optimal measurement strategies that satisfy some natural properties that make them both physically realizable and useful to a real-world verifier. We impose the following properties: (i) Locality: $\mathcal{S}$ contains only measurements corresponding to local observables, acting on a single copy of the output state; (ii) Projective measurement: $\mathcal{S}$ contains only binary-outcome, projective measurements, rather than more elaborate positive operator valued measures; and (iii) Trust: the physical operation of each measurement device is faithful to its mathematical description—it behaves as expected, without experimental error.

Thus, for multipartite states, we only consider strategies where each party locally performs a projective measurement on a single copy, and the parties accept or reject based on their collective measurement outcomes. We also highlight the trust requirement to distinguish from self-testing protocols [18–20].

Given this prescription and the set of physically motivated restrictions, we now derive the optimal verification strategy for some important classes of states. To illustrate our approach, we start with the case of a Bell state before generalizing to larger classes of states.

Bell state verification.—Consider the case of verifying the Bell state $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$. If we maintain a strategy where all measurements accept $|\Phi^+\rangle$ with certainty, then it must be the case that $\Omega|\Phi^+\rangle = |\Phi^+\rangle$. The optimization problem for the verifier-adversary pair is then given by Δ_ϵ,

$$\Delta_\epsilon = \max_{\Omega} \min_{\substack{\sigma \\ \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon}} \mathrm{tr}[\Omega(|\Phi^+\rangle\langle\Phi^+| - \sigma)]. \tag{4}$$

However, we show in the Supplemental Material [14] that it is never beneficial for the adversary to (a) choose a nonpure σ, or (b) to pick a σ such that $\langle\psi|\sigma|\psi\rangle < 1-\epsilon$. Rewrite $\sigma = |\psi_\epsilon\rangle\langle\psi_\epsilon|$, where $|\psi_\epsilon\rangle = \sqrt{1-\epsilon}|\Phi^+\rangle + \sqrt{\epsilon}|\psi^\perp\rangle$ for some state $|\psi^\perp\rangle$ such that $\langle\Phi^+|\psi^\perp\rangle = 0$. Then,

$$\Delta_\epsilon = \max_\Omega \min_{|\psi^\perp\rangle} \epsilon(\langle\Phi^+|\Omega|\Phi^+\rangle - \langle\psi^\perp|\Omega|\psi^\perp\rangle) - 2\sqrt{\epsilon(1-\epsilon)}\mathrm{Re}\langle\Phi^+|\Omega|\psi^\perp\rangle. \tag{5}$$

Given that $\Omega|\Phi^+\rangle = |\Phi^+\rangle$, we can simplify by noting that $\langle\Phi^+|\Omega|\Phi^+\rangle = 1$ and $\langle\Phi^+|\Omega|\psi^\perp\rangle = 0$. Thus,

$$\begin{aligned}\Delta_\epsilon &= \max_\Omega \min_{|\psi^\perp\rangle} \epsilon(1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle)\\ &= \epsilon(1 - \min_\Omega \max_{|\psi^\perp\rangle}\langle\psi^\perp|\Omega|\psi^\perp\rangle),\end{aligned} \tag{6}$$

where the verifier controls Ω and the adversary controls $|\psi^\perp\rangle$. Given that $|\Phi^+\rangle$ is itself an eigenstate of Ω, the worst-case scenario for the verifier is for the adversary to choose $|\psi^\perp\rangle$ as the eigenstate of Ω with the next largest eigenvalue. If we diagonalize Ω, we can write $\Omega = |\Phi^+\rangle\langle\Phi^+| + \sum_{j=1}^3 \nu_j|\psi_j^\perp\rangle\langle\psi_j^\perp|$, where $\langle\Phi^+|\psi_j^\perp\rangle = 0\ \forall j$. The adversary picks the state $|\psi_{\max}^\perp\rangle$ with corresponding eigenvalue $\nu_{\max} = \max_j \nu_j$. Now, consider the trace of Ω: if $\mathrm{tr}(\Omega) < 2$, then the strategy must be a convex combination of local projectors, at least one of which is rank 1. However, the only rank 1 projector that satisfies $P^+|\Phi^+\rangle = |\Phi^+\rangle$ is $P^+ = |\Phi^+\rangle\langle\Phi^+|$, which is nonlocal, and therefore $\mathrm{tr}(\Omega) \geq 2$. Combining this with the expression for Ω above gives $\mathrm{tr}(\Omega) = 1 + \sum_j \nu_j \geq 2$. It is always beneficial to the verifier to saturate this inequality, as any extra weight on the subspace orthogonal to $|\Phi^+\rangle$ can only increase the chance of being fooled by the adversary. Thus, the verifier is left with the optimization

$$\min \nu_{\max} = \min \max_k \nu_k, \qquad \sum_k \nu_k = 1. \tag{7}$$

This expression is optimized for $\nu_j = 1/3$, $j = 1, 2, 3$. In this case, $\Omega = \mathbb{1}/3$ on the subspace orthogonal to the state $|\Phi^+\rangle$. Then we can rewrite Ω as

$$\Omega = \frac{1}{3}(P_{XX}^+ + P_{-YY}^+ + P_{ZZ}^+), \tag{8}$$

where P_{XX}^+ is the projector onto the positive eigensubspace of the tensor product of Pauli matrices XX (and likewise for $-YY$ and ZZ). The operational interpretation of this optimal strategy is then explicit: for each copy of the state, the verifier randomly chooses a measurement setting from the set $\{XX, -YY, ZZ\}$ all with probability 1/3, and accepts only on receipt of outcome "+1" on all n measurements. Note that we could expand Ω differently, for example, by conjugating each term in the above expression by any local operator that leaves $|\Phi^+\rangle$ alone; the decomposition above is only one of a family of optimal strategies. As for scaling, we know that $\Delta_\epsilon = \epsilon(1-\nu_{\max}) = (2\epsilon/3)$, and the number of measurements needed to verify the Bell state $|\Phi^+\rangle$ is then $n_{\mathrm{opt}} = \{\ln[3/(3-2\epsilon)]\}^{-1}\ln(1/\delta) \approx (3/2\epsilon)\ln(1/\delta)$. Note that this is only worse than the optimal nonlocal strategy by a factor of 1.5.

In comparison, consider instead verifying a Bell state by performing a Clauser-Horne-Shimony-Holt test. Then, even in the case of trusted measurements, the total number of measurements scales like $O(1/\epsilon^2)$ [21], which is quadratically worse than the case of measuring the stabilizers $\{XX, -YY, ZZ\}$. This suboptimal scaling is shared by the known bounds for nonadaptive quantum state tomography with single-copy measurements in [12] and fidelity estimation in [13]. See [22–24] for further discussion of this scaling in tomography. Additionally, 2-qubit tomography potentially requires five times as many measurement settings. We also note that a similar quadratic improvement was derived in adaptive quantum state tomography in [25], in the sample-optimal tomographic scheme in [26], and in the quantum state certification scheme in [27]; however, the schemes therein assume access to either nonlocal or collective measurements.

Arbitrary states of two qubits.—The goal is unchanged for other pure states of two qubits: we seek strategies that accept the target state with certainty and hence achieve the asymptotic advantage outlined for Bell states above. It is not clear *a priori* that such a strategy exists for general states, in a way that is as straightforward as the previous construction. However, we show that for any 2-qubit state not only does such a strategy exist, but we can optimize within the family of allowable strategies and give an analytic expression with optimal constant factors.

We first remark that we can restrict to states of the form $|\psi_\theta\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ without loss of generality, as any state is locally equivalent to a state of this form, for some θ. Specifically, given any 2-qubit state $|\psi\rangle$ with optimal strategy Ω_{opt}, a locally equivalent state $(U\otimes V)|\psi\rangle$ has optimal strategy $(U\otimes V)\Omega_{\mathrm{opt}}(U\otimes V)^\dagger$. The proof of this statement can be found in the Supplemental Material [14]. Given the restriction to this family of states, we can now write down an optimal verification protocol.

Theorem 1.—Any optimal strategy for verifying a state of the form $|\psi_\theta\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ for $0 < \theta < (\pi/2)$, $\theta \neq (\pi/4)$ that accepts $|\psi_\theta\rangle$ with certainty and satisfies the properties of locality, trust, and projective measurement can be expressed as a strategy involving four measurement settings,

$$\begin{aligned}\Omega_{\mathrm{opt}} &= \alpha(\theta)P_{ZZ}^+\\ &\quad + \frac{1-\alpha(\theta)}{3}\sum_{k=1}^3[\mathbb{1} - (|u_k\rangle\otimes|v_k\rangle)(\langle u_k|\otimes\langle v_k|)],\end{aligned}$$

$$\text{for } \alpha(\theta) = \frac{2-\sin(2\theta)}{4+\sin(2\theta)}, \tag{9}$$

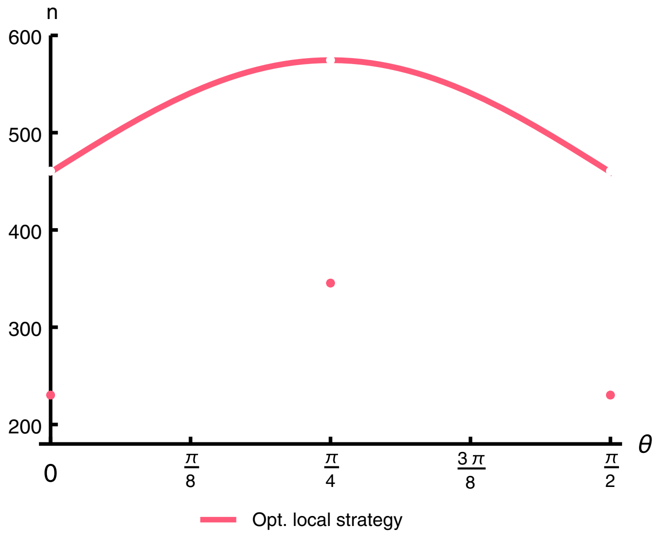

FIG. 1. The number of measurements needed to verify the state $|\psi_\theta\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$, as a function of θ, using the optimal strategy. [See Eq. (10).] Here, $1-\epsilon = 0.99$ and $1-\delta = 0.9$.

where P_{ZZ}^{+} is the projector onto the positive eigenspace of the Pauli operator ZZ, and the sets of states $\{|u_k\rangle\}$ and $\{|v_k\rangle\}$ are written explicitly in the Supplemental Material [14]. The number of measurements needed to verify to within infidelity ϵ and with power $1-\delta$ satisfies

$$n_{\text{opt}} \approx (2+\sin\theta\cos\theta)\epsilon^{-1}\ln\delta^{-1}. \qquad (10)$$

The proof of this Theorem is included in the Supplemental Material [14]. Note that the special cases for $|\psi_\theta\rangle$ where $\theta=0$, $\theta=(\pi/2)$, and $\theta=(\pi/4)$ are omitted from this theorem. In these cases, $|\psi_\theta\rangle$ admits a wider choice of measurements that accept with certainty. We have already treated the Bell state case $\theta=(\pi/4)$ above. In the other two cases, the state $|\psi_\theta\rangle$ is product and hence the globally optimal measurement, just projecting onto $|\psi_\theta\rangle$, is a valid local strategy. We note that this leads to a discontinuity in the number of measurements needed as a function of θ, for fixed ϵ (as seen in Fig. 1). This arises since our strategies are designed to have the optimal scaling $O(1/\epsilon)$ for fixed θ, achieved by having strategies that accept $|\psi\rangle$ with probability 1.

As for scaling, in Fig. 2, the number of measurements required to verify a particular 2-qubit state of this form, for three protocols, is shown. The optimal protocol derived here gives a marked improvement over the previously published bounds for both tomography [12] and fidelity estimation [13] for the full range of ϵ, for the given values of θ and δ. The asymptotic nature of the advantage for the protocol described here implies that the gap between the optimal scheme and tomography only grows as the requirement on ϵ becomes more stringent. Note also that the optimal local strategy is only marginally worse than the best possible strategy of just projecting onto $|\psi\rangle$.

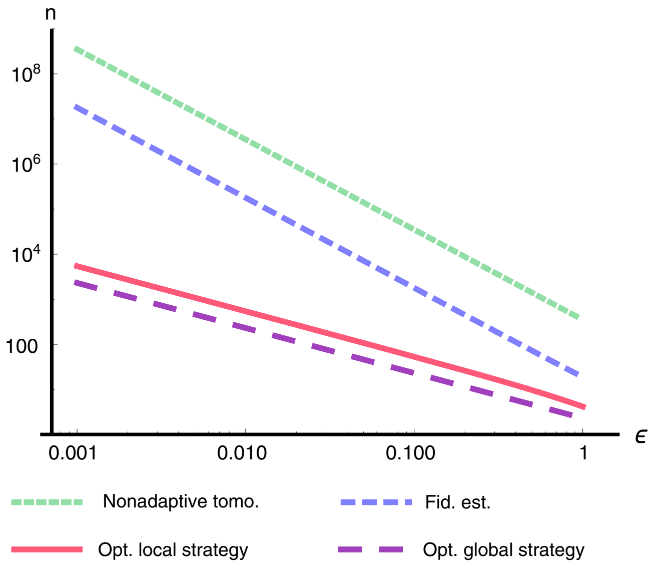

FIG. 2. A comparison of the total number of measurements required to verify to fidelity $1-\epsilon$ for the strategy derived here versus the known bounds for estimation up to fidelity $1-\epsilon$ using nonadaptive tomography in [12], the fidelity estimation protocol in [13], and the globally optimal strategy given by projecting onto $|\psi\rangle$. Here, $1-\delta = 0.9$ and $\theta = (\pi/8)$.

Stabilizer states.—Additionally, it is shown in the Supplemental Material [14] that we can construct a strategy with the same asymptotic advantage for any stabilizer state, by drawing measurements from the stabilizer group (where now we only claim optimality up to constant factors). The derivation is analogous to that for the Bell state above, and given that the Bell state is itself a stabilizer state, the strategy above is a special case of the stabilizer strategy discussed below. For a state of N qubits, a viable strategy constructed from stabilizers must consist of at least the N stabilizer generators of $|\psi\rangle$. This is because a set of $k<N$ stabilizers stabilizes a subspace of dimension at least 2^{N-k}, and so, in this case, there always exists at least one orthogonal state to $|\psi\rangle$ accessible to the adversary that fools the verifier with certainty. In this minimal case, the number of required measurements is $n_{\text{opt}}^{\text{s.g.}} \approx N\epsilon^{-1}\ln\delta^{-1}$, with this bound saturated by measuring all stabilizer generators with equal weight. Conversely, constructing a measurement strategy from the full set of 2^N-1 linearly independent stabilizers requires a number of measurements $n_{\text{opt}}^{\text{stab}} \approx [(2^N-1)/2^{(N-1)}]\epsilon^{-1}\ln\delta^{-1}$, again with this bound saturated by measuring each stabilizer with equal weight. For growing N, the latter expression for the number of measurements is bounded from above by $2\epsilon^{-1}\ln\delta^{-1}$, which implies that there is a local strategy for any stabilizer state, of an arbitrary number of qubits, which requires, at most, twice as many measurements as the optimal nonlocal strategy. Note that this strategy may not be exactly optimal; for example, the state $|00\rangle$ is also a stabilizer state, and in this case, applying the measurement $|00\rangle\langle 00|$ is both locally

implementable and provably optimal. Thus, the exactly optimal strategy may depend more precisely on the structure of the individual state itself. However, the stabilizer strategy is only inferior by a small constant factor. In comparison to the latter strategy constructed from every stabilizer, the former strategy constructed from only the N stabilizer generators of $|\psi\rangle$ has scaling that grows linearly with N. Thus, there is ultimately a trade-off between number of measurement settings and total number of measurements required to verify within a fixed fidelity.

In principle, the recipe derived here to extract the optimal strategy for a state of two qubits can be applied to any pure state. However, we anticipate that deriving this strategy, including correct constants, may be somewhat involved (both analytically and numerically) for states of greater numbers of qubits.

The authors thank Jeremy Adcock, Sam Morley-Short, Tony Short, and Chris Sparrow for helpful discussions. We also thank Borivoje Dakic for pointing out [28], and Otfried Guehne for pointing out [29,30]. S. P. was supported by the Bristol Quantum Engineering Centre for Doctoral Training, EPSRC Grant No. EP/L015730/1. A. M. was supported by EPSRC Early Career Fellowship EP/L021005/1. No new data were created during this study.

Note added.—Recently, we became aware of [28] which, among other results, applies a similar protocol to the Bell state verification strategy in the context of entanglement detection. We were also notified that the strategy in Eq. (9), which we prove optimal for verification, has previously been studied in two different contexts: in Ref. [29] as an "optimal pseudomixture" of pure states, and in Ref. [30] as a method for entanglement detection. Finally [31,32] have been brought to our attention; these references give local verification protocols for graphs and hypergraph states, respectively.

[*] sam.pallister@bristol.ac.uk
[†] n.linden@bristol.ac.uk
[‡] ashley.montanaro@bristol.ac.uk

[1] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al Kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Nature (London) **438**, 643 (2005).

[2] J. Carolan, J. D. A. Meinecke, P. J. Shadbolt, N. J. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O'Brien, J. C. F. Matthews, and A. Laing, Nat. Photonics **8**, 621 (2014).

[3] A. Laing and J. L. O'Brien, arXiv:1208.2868.

[4] A. I. Lvovsky and M. G. Raymer, Rev. Mod. Phys. **81**, 299 (2009).

[5] M. Bellini, A. S. Coelho, S. N. Filippov, V. I. Man'ko, and A. Zavatta, Phys. Rev. A **85**, 052129 (2012).

[6] G. G. Amosov, Y. A. Korennoy, and V. I. Man'ko, Phys. Rev. A **85**, 052119 (2012).

[7] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, New J. Phys. **14**, 095022 (2012).

[8] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Phys. Rev. Lett. **105**, 150401 (2010).

[9] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. **1**, 149 (2010).

[10] G. Tóth and O. Gühne, Phys. Rev. Lett. **94**, 060501 (2005).

[11] G. Tóth and O. Gühne, Phys. Rev. A **72**, 022340 (2005).

[12] T. Sugiyama, P. S. Turner, and M. Murao, Phys. Rev. Lett. **111**, 160406 (2013).

[13] S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett. **106**, 230501 (2011).

[14] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.120.170502 for further discussion and proofs.

[15] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).

[16] J. Calsamiglia and N. Lütkenhaus, Appl. Phys. B **72**, 67 (2001).

[17] F. Ewert and P. van Loock, Phys. Rev. Lett. **113**, 140403 (2014).

[18] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[19] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A **45**, 455304 (2012).

[20] T. H. Yang and M. Navascués, Phys. Rev. A **87**, 050102 (2013).

[21] T. Sugiyama, *Finite Sample Analysis in Quantum Estimation* (Springer, New York, 2014).

[22] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Phys. Rev. Lett. **107**, 210404 (2011).

[23] C. Ferrie and R. Blume-Kohout, Phys. Rev. Lett. **116**, 090407 (2016).

[24] G. I. Struchalin, I. A. Pogorelov, S. S. Straupe, K. S. Kravtsov, I. V. Radchenko, and S. P. Kulik, Phys. Rev. A **93**, 012103 (2016).

[25] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg, Phys. Rev. Lett. **111**, 183601 (2013).

[26] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, in *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing—STOC 2016* (ACM Press, New York, 2016) p. 913.

[27] C. Bădescu, R. O'Donnell, and J. Wright, arXiv:1708.06002.

[28] A. Dimić and B. Dakić, arXiv:1705.06719.

[29] A. Sanpera, R. Tarrach, and G. Vidal, Phys. Rev. A **58**, 826 (1998).

[30] O. Guehne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).

[31] M. Hayashi and T. Morimae, Phys. Rev. Lett. **115**, 220502 (2015).

[32] T. Morimae, Y. Takeuchi, and M. Hayashi, Phys. Rev. A **96**, 062321 (2017).