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, UK*

[2] *Quantum Engineering Centre for Doctoral Training, University of Bristol, UK*

(Dated: September 11, 2017)

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 characterise 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 amongst local verification strategies for two 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, non-adaptive and non-collective measurements only incurs a constant-factor penalty over a strategy without these restrictions.

Efficient and reliable quantum state preparation is a necessary step in the maturation of all quantum technologies. However, characterisation and verification of such devices is typically a time-consuming and computationally difficult process. For example, tomographic reconstruction of a state of 8 ions required taking $\sim 650,000$ measurements over 10 hours, and a statistical analysis that took far longer [1]; verification of a state of a small number of qubits in photonics is similarly challenging [2, 3]. One may instead resort to non-tomographic methods to verify that a device reliably outputs a particular state, but such methods typically either: (a) assume that the verifier already knows that the output state is within some special family of states, for example in compressed sensing [4, 5] or matrix product state tomography [6]; or (b) extract only partial information about the state, such as when estimating entanglement witnesses [7, 8].

Here, we derive the optimal local verification strategy for common entangled states. We also compare its performance to the bounds for non-adaptive quantum state tomography in [9] and the fidelity estimation protocol in [10]. In particular, we demonstrate non-adaptive verification strategies for arbitrary two-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 are required for these previous protocols. Moreover, the requirement that the measurements be local incurs only a constant factor penalty over the best non-local 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 rather than 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 as a hypothesis test with some finite statistical power. 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 typically 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 to 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 equal to $|\psi\rangle$, 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's goal is to determine which is the case with worst-case failure probability δ.

The verification 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 in the case that $\sigma_i = |\psi\rangle\langle\psi|$, $\forall i$ (i.e. that $|\psi\rangle$ is in the "pass" eigenspace of every projector $P_j \in \mathcal{S}$). This may appear to be a prohibitively strong constraint,

* sam.pallister@bristol.ac.uk

† N.Linden@bristol.ac.uk

‡ ashley.montanaro@bristol.ac.uk

but we later demonstrate that it is both achievable for the sets of states we consider and is always asymptotically favourable to the verifier.

The maximal probability that the verifier passes on copy i is

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

where $\Omega_i = \sum_j \mu_j^i P_j$. However, the verifier seeks to minimise 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 optimisation is

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

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:

A. *Non-adaptivity.* 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.

B. *Future-proofing.* The strategy prescription is independent of the infidelity ϵ, and gives a viable strategy for any choice of ϵ. Thus an experimentalist verifying a state $|\psi\rangle$ is able to arbitrarily decrease the infidelity ϵ within which verification succeeds by simply taking more total measurements according to the strategy prescription, rather than modifying the details of the strategy itself. Also, 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 non-adaptive 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 that strategies of this type 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 non-local, adaptive or collective measurements) would yield only at most constant-factor improvements.

It is straightforward to show, given no constraints on the verifier's measurement prescription, that the optimal strategy is to just project on to $|\psi\rangle$. In this case, the fewest number of measurements needed to verify to confidence $1-\delta$ and fidelity $1-\epsilon$ is $n_{opt} = \frac{-1}{\ln(1-\epsilon)} \ln \frac{1}{\delta} \approx \frac{1}{\epsilon} \ln \frac{1}{\delta}$ (see the Supplemental Material). However, in general the projector $|\psi\rangle\langle\psi|$ will be non-local. Non-local measurements have the disadvantage of being harder to implement experimentally. This is particularly problematic in quantum optics, where deterministic, unambiguous discrimination of a complete set of Bell states is impossible [11–13]. 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, just the probability of successfully carrying out the protocol decreases exponentially with the number of measurements. Instead, we seek optimal measurement strategies that satisfy some natural properties that make them both physically realisable and useful to a real-world verifier. We optimise over strategies with the following properties:

1. *Locality.* $\mathcal{S}$ contains only measurements corresponding to local observables, acting on a single copy of the output state.

2. *Projective measurement.* $\mathcal{S}$ contains only binary-outcome, projective measurements, rather than more elaborate POVMs.

3. *Trust.* The physical operation of each measurement device is faithful to its mathematical description; it behaves exactly as expected.

We highlight the trust requirement for two reasons: first, in order to distinguish from self-testing protocols [14–16], where this property is not assumed; and second, to clarify that we assume that there is no experimental error in the measurement process.

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 generalising to larger classes of states.

Bell state verification. Consider the case of verifying the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. 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 optimisation problem for the verifier-adversary pair is then given by Δ_ϵ:

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

However, it is shown in the Supplemental Material that it is never beneficial for the adversary to: (a) choose a non-pure 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 has access to 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 diagonalise 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 non-local; 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 optimisation

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

It is clear that this expression is optimised for $\nu_j = \frac{1}{3}, j = 1, 2, 3$. In this case, $\Omega = \frac{\mathbb{1}}{3}$ 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 $\frac{1}{3}$, and accepts only on receipt of outcome "+1" on all n measurements. Note that we could have expanded 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 $\Delta_\epsilon = \epsilon(1 - \nu_{\max}) = \frac{2\epsilon}{3}$, and the number of measurements needed to verify the Bell state $|\Phi^+\rangle$ is then $n_{opt} = \left[\ln\left(\frac{3}{3-2\epsilon}\right)\right]^{-1} \ln\frac{1}{\delta} \approx \frac{3}{2\epsilon}\ln\frac{1}{\delta}$. Note that this is only worse than the optimal non-local strategy by a factor of 1.5.

In comparison, consider instead verifying a Bell state by performing a CHSH test. Then even in the case of trusted measurements, the total number of measurements scales like $O\left(\frac{1}{\epsilon^2}\right)$ [17], which is quadratically worse than the case of measuring the stabilizers $\{XX, -YY, ZZ\}$. This suboptimal scaling is shared by the known bounds for non-adaptive quantum state tomography with single-copy measurements in [9] and fidelity estimation in [10]. See [18–20] for further discussion of this scaling in tomography. Additionally, two-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 [21], in the sample-optimal tomographic scheme in [22] and in the quantum state certification scheme in [23]; however, the schemes therein assume access to either non-local 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 from the outset that such a strategy can be constructed for general states, in a way that is as straightforward as the previous construction. However, we show that for any two-qubit state not only does such a strategy exist, but we can optimise 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 two qubit state $|\psi\rangle$ with optimal strategy Ω_{opt}, a locally equivalent state $(U \otimes V)|\psi\rangle$ has optimal strategy $(U \otimes V)\Omega_{opt}(U \otimes V)^\dagger$. The proof of this statement can be found in the Supplemental Material. 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 $0 < \theta < \frac{\pi}{2}$, $\theta \neq \frac{\pi}{4}$ 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:*

$$\begin{aligned}\Omega_{opt} &= \alpha(\theta)P_{ZZ}^+ \\ &\quad + \frac{1-\alpha(\theta)}{3}\sum_{k=1}^3 \left[\mathbb{1} - (|u_k\rangle \otimes |v_k\rangle)(\langle u_k| \otimes \langle v_k|)\right], \\ &\text{for } \alpha(\theta) = \frac{2-\sin(2\theta)}{4+\sin(2\theta)},\end{aligned} \tag{9}$$

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. The number of measurements needed to verify to

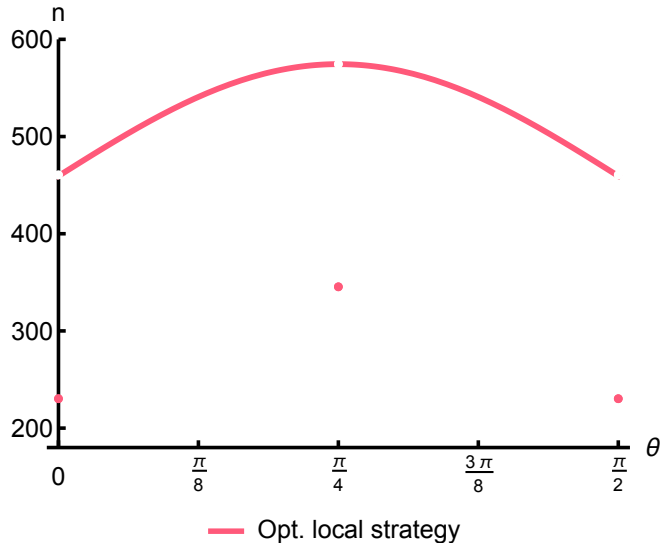

FIG. 1. The number of measurements needed to verify the state $|\psi_\theta\rangle = \sin\theta\,|00\rangle + \cos\theta\,|11\rangle$, as a function of θ, using the optimal strategy. See Eq. 10. Here, $1-\epsilon = 0.99$ and $1-\delta = 0.9$.

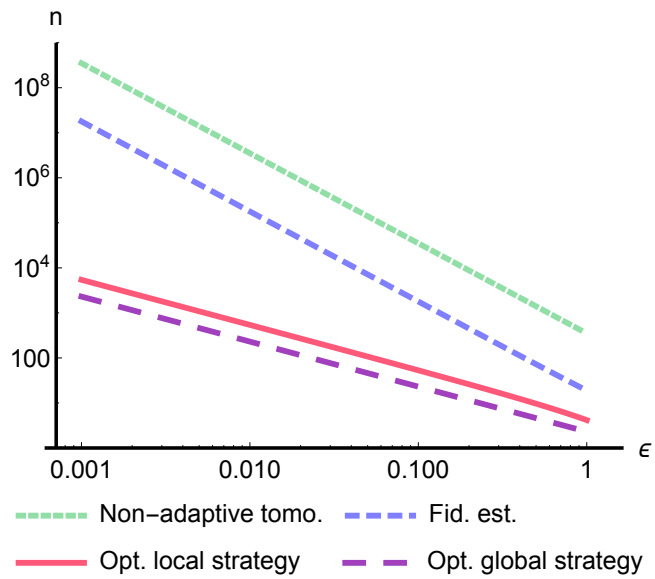

FIG. 2. A comparison of the total number of measurements required to verify to fidelity $1-\epsilon$ for the strategy derived here, versus the known bounds for estimation up to fidelity $1-\epsilon$ using non-adaptive tomography in [9] and the fidelity estimation protocol in [10], and the globally optimal strategy given by projecting onto $|\psi\rangle$. Here, $1-\delta = 0.9$ and $\theta = \frac{\pi}{8}$.

within infidelity ϵ and with power $1-\delta$ satisfies

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

Proof sketch. The full proof is included in the Supplemental Material, and we give a sketch here. The basic principle is to consider the most general form that a measurement strategy Ω could take, to narrow down its form in a succession of steps, and then to show that there is an explicit convex combination of projectors of the desired form that equates to this optimised Ω. The first step is to rule out families of measurements that are forbidden while maintaining that the strategy accepts $|\psi\rangle$ with certainty (analogously to the remark regarding rank 1 projectors in the Bell state case, above). The second step is to note that, given a strategy for verifying the state $|\psi\rangle$ and an operator U under which $|\psi\rangle$ is invariant, conjugating the strategy by U produces a valid strategy of equal performance. As an example, the state $|\psi_\theta\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ is invariant under swapping of the first and second qubit, which implies that the "swap-averaged" strategy $\Omega' = \frac{1}{2}(\Omega + \Omega^{SWAP})$ performs at least as well at verifying $|\psi\rangle$ as Ω. Moreover, we can average the strategy over multiple choices of U and be left with a compound strategy that is at least as good, which reduces the possible form for Ω considerably. We can then explicitly parameterise the resulting strategy, and optimise to derive maximum benefit to the verifier. For a two-qubit state of the form $|\psi_\theta\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$, this is enough to narrow down Ω to the restricted form above. □

Note that the special cases where the state $|\psi_\theta\rangle$ takes a particular form, $\theta = 0$, $\theta = \frac{\pi}{2}$ and $\theta = \frac{\pi}{4}$ are omitted from this theorem. In these cases, the state admits a wider choice of measurements that accept $|\psi_\theta\rangle$ with certainty. We have already treated the Bell state case $\theta = \frac{\pi}{4}$ 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 may be seen in Fig. 1). This arises since our strategies are designed to have the optimal scaling $\left(O\left(\frac{1}{\epsilon}\right)\right)$ 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 two-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 [9] and fidelity estimation [10] 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 verification scheme and quantum state 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 $|\psi\rangle$.

Stabilizer states. Additionally, it is shown in the Supplemental Material 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 discussed above for the Bell state. 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 $n_{opt}^{s.g.} \approx N\epsilon^{-1}\ln\delta^{-1}$, 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 $n_{opt}^{stab} \approx \frac{2^N-1}{2^{(N-1)}}\epsilon^{-1}\ln\delta^{-1}$, 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 non-local strategy. In comparison, 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 this case.

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 the optimal 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. SP was supported by the Bristol Quantum Engineering Centre for Doctoral Training, EPSRC grant EP/L015730/1. AM was supported by EPSRC Early Career Fellowship EP/L021005/1. No new data were created during this study.

[1] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chekal Kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Nature **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, Nature Photonics **8**, 621 (2014).
[3] A. Laing and J. L. O'Brien, arXiv:1208.2868 (2012).
[4] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, New Journal of Physics **14**, 095022 (2012).
[5] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Physical Review Letters **105**, 150401 (2010).
[6] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nature Communications **1**, 149 (2010).
[7] G. Tóth and O. Gühne, Physical Review Letters **94**, 060501 (2005).
[8] G. Tóth and O. Gühne, Physical Review A **72**, 022340 (2005).
[9] T. Sugiyama, P. S. Turner, and M. Murao, Physical Review Letters **111**, 160406 (2013).
[10] S. T. Flammia and Y.-K. Liu, Physical Review Letters **106**, 230501 (2011).
[11] L. Vaidman and N. Yoran, Physical Review A **59**, 116 (1999).
[12] J. Calsamiglia and N. Lütkenhaus, Applied Physics B **72**, 67 (2001).
[13] F. Ewert and P. van Loock, Physical Review Letters **113**, 140403 (2014).
[14] D. Mayers and A. Yao, Quantum Information & Computation **4**, 273 (2004).
[15] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical **45**, 455304 (2012).
[16] T. H. Yang and M. Navascués, Physical Review A **87**, 050102 (2013).
[17] T. Sugiyama, *Finite Sample Analysis in Quantum Estimation* (Springer, 2014).
[18] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Physical Review Letters **107**, 210404 (2011).
[19] C. Ferrie and R. Blume-Kohout, Physical Review Letters **116**, 090407 (2016).
[20] G. I. Struchalin, I. A. Pogorelov, S. S. Straupe, K. S. Kravtsov, I. V. Radchenko, and S. P. Kulik, Physical Review A **93**, 012103 (2016).
[21] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg, Physical Review Letters **111**, 183601 (2013).
[22] 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, New York, USA, 2016) pp. 913–925.
[23] C. Bădescu, R. O'Donnell, and J. Wright, arXiv:1708.06002 (2017).
[24] M. Hein, *Entanglement in graph states*, Ph.D. thesis, University of Innsbruck (2005).
[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, 2006).

Supplemental Material: Optimal verification of entangled states with local measurements

Appendix A: Quantum state verification

We first set up a formal framework for general state verification protocols. We assume that we have access to a device $\mathcal{D}$ that is supposed to produce copies of a state $|\psi\rangle$. However, $\mathcal{D}$ might not work correctly, and actually produces (potentially mixed) states $\sigma_1, \sigma_2, \ldots$ such that σ_i might not be equal to $|\psi\rangle\langle\psi|$. In order to distinguish this from the case where the device works correctly by making a reasonable number of uses of $\mathcal{D}$, we need to have a promise that these states are sufficiently far from $|\psi\rangle$. So we are led to the following formulation of our task:

Distinguish between the following two cases:

(a). **(Good)** $\sigma_i = |\psi\rangle\langle\psi|$ for all i;

(b). **(Bad)** For some fixed ϵ, $F(|\psi\rangle, \sigma_i) := \langle\psi|\sigma_i|\psi\rangle \leq 1 - \epsilon$ for all i.

Given a verifier with access to a set of available measurements $\mathcal{S}$, the protocols we consider for completing this task are of the following form:

Protocol Quantum state verification

```
for i = 1 to n do
    Two-outcome measurement M_i ∈ S on σ_i, where M_i's outcomes are associated with "pass" and "fail"
    if "fail" is returned then
        Output "reject"
Output "accept"
```

We impose the conditions that in the good case, the protocol accepts with certainty, whereas in the bad case, the protocol accepts with probability at most δ; we call $1 - \delta$ the *statistical power* of the protocol. We then aim to find a protocol that minimises n for a given choice of $|\psi\rangle$, ϵ and $\mathcal{S}$, such that these constraints are satisfied. Insisting that the protocol accepts in the good case with certainty implies that all measurements in $\mathcal{S}$ are guaranteed to pass in this case. This is a desirable property in itself, but one could consider more general non-adaptive protocols where measurements do not output "pass" with certainty on $|\psi\rangle$, and the protocol determines whether to accept based on an estimator constructed from the relative frequency of "pass" and "fail" outcomes across all n copies. We show in Appendix E that this class of protocols has quadratically worse scaling in ϵ than protocols where each measurement passes with certainty on $|\psi\rangle$.

We make the following observations about this framework:

1. Given no restrictions on M_i, the optimal protocol is simply for each measurement to project onto $|\psi\rangle$. In fact, this remains optimal even over the class of more general protocols making use of adaptivity or collective measurements. One can see this as follows: if a two-outcome measurement M (corresponding to the whole protocol) is described by measurement operators P (accept) and $I - P$ (reject), then if M accepts $|\psi\rangle^{\otimes n}$ with certainty, we must have $P = |\psi\rangle\langle\psi|^{\otimes n} + P'$ for some residual positive semidefinite operator P'. Then replacing P with $|\psi\rangle\langle\psi|^{\otimes n}$ gives at least as good a protocol, as the probability of accepting $|\psi\rangle$ remains 1, while the probability of accepting other states cannot increase.

   The probability of acceptance in the bad case after n trials is then at most $(1-\epsilon)^n$, so it is sufficient to take

   $$n \geq \frac{\ln \delta^{-1}}{\ln((1-\epsilon)^{-1})} \approx \epsilon^{-1} \ln \delta^{-1} \tag{S1}$$

   to achieve statistical power $1 - \delta$. This will be the yardstick against which we will compare our more restricted protocols below.

2. We assume that the states σ_i are independently and adversarially chosen. This implies that if (as we will consider below) $\mathcal{S}$ contains only projective measurements and does not contain the measurement projecting onto $|\psi\rangle\langle\psi|$, it is necessary to choose the measurement M_i at random from $\mathcal{S}$ and unknown to the adversary. Otherwise, we could be fooled with certainty by the adversary choosing σ_i to have support only in the "pass" eigenspace of M_i for each copy i.

3. We can be explicit about the optimisation needed to derive the optimal protocol in this adversarial setting. As protocols of the above form reject whenever a measurement fails, the adversary's goal at the i'th step is to maximise the probability that the measurement M_i at that step passes on σ_i. If the j'th measurement setting in $\mathcal{S}$, M^j, is picked from $\mathcal{S}$ at step i with probability μ_j^i, the largest possible overall probability of passing for copy i is

$$\Pr[\text{Pass on copy } i] = \max_{\sigma_i, \langle\psi|\sigma_i|\psi\rangle \leq 1-\epsilon} \sum_j \mu_j^i \operatorname{tr}(P_j \sigma_i), \tag{S2}$$

where we denote the corresponding "pass" projectors P_j. We can write $\Omega_i = \sum_j \mu_j^i P_j$, and then

$$\Pr[\text{Pass on copy } i] = \max_{\sigma, \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon} \operatorname{tr}(\Omega_i \sigma). \tag{S3}$$

As the verifier, we wish to minimise this expression over all Ω_i, so we end up with a final expression that does not depend on i. This leads us to infer that optimal protocols of this form can be assumed to be non-adaptive in two senses: they do not depend on the outcome of previous measurements (which is clear, as the protocol rejects if it ever sees a "fail" outcome); and they also do not depend on the measurement choices made previously.

Therefore, in order to find an optimal verification protocol, our task is to determine

$$\min_{\Omega} \max_{\sigma, \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon} \operatorname{tr}(\Omega\sigma), \tag{S4}$$

where Ω is an operator of the form $\Omega = \sum_j \mu_j P_j$ for $P_j \in \mathcal{S}$ and some probability μ_j. We call such operators *strategies*. If $\mathcal{S}$ contained all measurement operators (or even all projectors), Ω would be an arbitrary operator satisfying $0 \leq \Omega \leq I$. However, this notion becomes nontrivial when one considers restrictions on $\mathcal{S}$. Here, we focus on the experimentally motivated case where $\mathcal{S}$ contains only projective measurements that can be implemented via local operations and classical postprocessing.

4. In a non-adversarial scenario, it may be acceptable to fix the measurements in Ω in advance, with appropriate frequencies μ_j. Then, given n, a strategy $\Omega = \sum_j \mu_j P_j$ corresponds to a protocol where for each j we deterministically make $\mu_j n$ measurements $\{P_j, I - P_j\}$. For large n, and fixed $\sigma_i = \sigma$, this will achieve similar performance to the above protocol.

5. More complicated protocols with adaptive or collective measurements, or measurements with more than two outcomes, cannot markedly improve on the strategies derived here. We do not treat these more general strategies explicitly, but note that the protocols we will describe based on local projective measurements already achieve the globally optimal bound (S1) up to constant factors, so any gain from these more complex approaches would be minor.

Appendix B: Verification strategy optimisation

In this appendix, we simplify the form of the optimisation in S4 using the strategy requirements outlined previously. We start by making the following useful observation:

Lemma 2. *We can assume without loss of generality that, in (S4), σ is pure.*

Proof. Assume the adversary chooses a fixed density matrix σ, which is globally optimal: it forces the verifier to accept σ with the greatest probability among states σ such that $\langle\psi|\sigma|\psi\rangle \coloneqq r \leq 1-\epsilon$. The probability of accepting this σ given strategy Ω is then

$$\Pr[\text{Accept } \sigma] = \operatorname{tr}(\Omega\sigma). \tag{S1}$$

We have asserted that Ω accepts $|\psi\rangle$ with certainty: $\langle\psi|\Omega|\psi\rangle = 1$. However, for this to be the case Ω must have $|\psi\rangle$ as an eigenstate with eigenvalue 1; thus we can write

$$\Omega = |\psi\rangle\langle\psi| + \sum_j c_j |\psi_j^\perp\rangle\langle\psi_j^\perp| \tag{S2}$$

where the states $\{|\psi_j^\perp\rangle\}$ are a set of mutually orthogonal states orthogonal to $|\psi\rangle$. Then

$$\Pr[\text{Accept } \sigma] = \langle\psi|\sigma|\psi\rangle + \sum_j c_j \langle\psi_j^\perp|\sigma|\psi_j^\perp\rangle \tag{S3}$$

$$= r + \sum_j c_j \langle\psi_j^\perp|\sigma|\psi_j^\perp\rangle. \tag{S4}$$

We can write

$$\sigma = a|\psi\rangle\langle\psi| + b\sigma^\perp + c|\psi\rangle\langle\Phi^\perp| + c^*|\Phi^\perp\rangle\langle\psi|, \tag{S5}$$

where $\sigma^\perp$ is a density matrix entirely supported in the subspace spanned by the states $|\psi_j^\perp\rangle$, and $|\Phi^\perp\rangle$ is a vector in the subspace spanned by $|\psi_j^\perp\rangle$. We know that $a = r$ as $\langle\psi|\sigma|\psi\rangle = r$, and $b = 1 - r$ as $\mathrm{tr}(\sigma) = 1$. Now, note that the probability of accepting σ does not depend on the choice of $|\Phi^\perp\rangle$. Thus $\mathrm{tr}(\Omega\sigma)$ is maximised when $\sigma^\perp = |\psi_{max}^\perp\rangle\langle\psi_{max}^\perp|$, where $|\psi_{max}^\perp\rangle$ is the orthogonal state in the spectral decomposition of Ω with largest eigenvalue, c_{max}. Thus

$$\max_\sigma \mathrm{tr}(\Omega\sigma) = r + (1-r)c_{max}, \tag{S6}$$

which is achieved by any density matrix of the form

$$\sigma = r|\psi\rangle\langle\psi| + (1-r)|\psi_{max}^\perp\rangle\langle\psi_{max}^\perp| + c|\psi\rangle\langle\Phi^\perp| + c^*|\Phi^\perp\rangle\langle\psi|. \tag{S7}$$

Note that the pure state $\sigma = |\phi\rangle\langle\phi|$ for $|\phi\rangle = \sqrt{r}|\psi\rangle + \sqrt{1-r}|\psi_{max}^\perp\rangle$ is of this form, and so we can assume that the adversary makes this choice. □

Given that the state σ can be taken to be pure and that the fidelity $F(|\psi\rangle, \sigma) \leq 1 - \epsilon$, we write $\sigma = |\psi_{\bar\epsilon}\rangle\langle\psi_{\bar\epsilon}|$, where $|\psi_{\bar\epsilon}\rangle := \sqrt{1-\bar\epsilon}|\psi\rangle + \sqrt{\bar\epsilon}|\psi^\perp\rangle$ and $\langle\psi|\psi^\perp\rangle = 0$, for some $\bar\epsilon \geq \epsilon$ chosen by the adversary, to be optimised later. Denote

$$\min_\Omega \max_{\substack{\sigma \\ \langle\psi|\sigma|\psi\rangle \leq 1-\epsilon}} \mathrm{tr}(\Omega\sigma) := 1 - \Delta_\epsilon. \tag{S8}$$

Then the optimisation problem becomes to determine Δ_ϵ, where

$$\Delta_\epsilon = \max_\Omega \min_{|\psi^\perp\rangle, \bar\epsilon \geq \epsilon} \bar\epsilon(1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle) - 2\sqrt{\bar\epsilon(1-\bar\epsilon)}\mathrm{Re}(\langle\psi|\Omega|\psi^\perp\rangle) \tag{S9}$$

$$\text{and } \Omega|\psi\rangle = |\psi\rangle. \tag{S10}$$

This expression can be simplified given that $\Omega|\psi\rangle = |\psi\rangle$. In particular, we then know that $\langle\psi^\perp|\Omega|\psi\rangle = 0$ for any choice of orthogonal state $|\psi^\perp\rangle$. Thus the term $\sqrt{\bar\epsilon(1-\bar\epsilon)}\mathrm{Re}(\langle\psi|\Omega|\psi^\perp\rangle)$ automatically vanishes. We are then left with the optimisation

$$\Delta_\epsilon = \max_\Omega \min_{|\psi^\perp\rangle, \bar\epsilon \geq \epsilon} \bar\epsilon(1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle), \tag{S11}$$

$$\text{where } \Omega|\psi\rangle = |\psi\rangle.$$

As for the optimisation of $\bar\epsilon$, note that it is the goal of the adversary to make Δ_ϵ as small as possible; and so they are obliged to set $\bar\epsilon = \epsilon$. Then the optimisation becomes

$$\Delta_\epsilon = \epsilon \max_\Omega \min_{|\psi^\perp\rangle}(1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle), \tag{S12}$$

$$\text{where } \Omega|\psi\rangle = |\psi\rangle.$$

Note that this expression implies that any Ω where $\Omega|\psi\rangle = |\psi\rangle$ automatically satisfies the *future-proofing* property: firstly that Ω is independent of ϵ, but also that the strategy must be viable for any choice of ϵ (i.e. there must not be a choice of ϵ where $\Delta_\epsilon = 0$). For an initial choice $\Delta_\epsilon > 0$, we have that $1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle > 0$ and so $\Delta_{\epsilon'} > 0$ for any $0 < \epsilon' < \epsilon$. Thus the verifier is free to decrease ϵ arbitrarily without fear of the strategy failing. Note also that this condition may not be automatically guaranteed if the verifier chooses an Ω such that $\Omega|\psi\rangle \neq |\psi\rangle$.

Regarding the optimisation problem in S12, for an arbitrary state $|\psi\rangle$ on n qubits it is far from clear how to: (a) construct families of viable Ω (built from local projective measurements) that accept $|\psi\rangle$ with certainty; (b) to then solve this optimisation problem over those families of Ω. For the remainder of this work, we focus on states of particular experimental interest where we can solve the problem: arbitrary states of 2 qubits, and stabilizer states.

Appendix C: States of two qubits

We now derive the optimal verification strategy for an arbitrary pure state of two qubits. We first give the proof of the statement in the main text that optimal strategies for locally equivalent states are easily derived by conjugating the strategy with the local map that takes one state to the other. Hence, we can restrict our consideration to verifying states of the form $|\psi\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ without loss of generality. Specifically:

Lemma 3. *Given any two qubit state $|\psi\rangle$ with optimal strategy Ω_{opt}, a locally equivalent state $(U\otimes V)|\psi\rangle$ has optimal strategy $(U\otimes V)\Omega_{opt}(U\otimes V)^\dagger$.*

Proof. We must show that strategy $\Omega' = (U\otimes V)\Omega_{opt}(U\otimes V)^\dagger$ is both a valid strategy, and is optimal for verifying $|\psi'\rangle = (U\otimes V)|\psi\rangle$.
Validity: If $\Omega_{opt} = \sum_j \mu_j P_j$ is a convex combination of local projectors, then so is Ω':

$$\begin{aligned}\Omega' = (U\otimes V)\Omega(U\otimes V)^\dagger &= \sum_j \mu_j (U\otimes V)P_j(U\otimes V)^\dagger \\ &= \sum_j \mu_j P_j'. \end{aligned} \tag{S1}$$

Also, if $\Omega_{opt}|\psi\rangle = |\psi\rangle$ then $\Omega'|\psi'\rangle = |\psi'\rangle$:

$$\begin{aligned}\Omega_{opt}|\psi\rangle = |\psi\rangle &\Rightarrow (U\otimes V)\Omega|\psi\rangle = p_{opt}(U\otimes V)|\psi\rangle \\ &\Rightarrow (U\otimes V)\Omega(U\otimes V)^\dagger(U\otimes V)|\psi\rangle = (U\otimes V)|\psi\rangle \\ &\Rightarrow \Omega'|\psi'\rangle = |\psi'\rangle.\end{aligned} \tag{S2}$$

Optimality: The performance of a strategy is determined by the maximum probability of accepting an orthogonal state $|\psi^\perp\rangle$. For the strategy-state pairs $(\Omega_{opt}, |\psi\rangle)$ and $(\Omega', |\psi'\rangle)$, we denote this parameter q_{opt} and q', respectively. Then

$$q_{opt} = \max_{|\psi^\perp\rangle} \langle\psi^\perp|\Omega_{opt}|\psi^\perp\rangle = \max_{|\phi\rangle, \langle\psi|\phi\rangle=0} \langle\phi|\Omega_{opt}|\phi\rangle \tag{S3}$$

$$= \max_{(U\otimes V)|\phi\rangle, \langle\psi|(U\otimes V)^\dagger(U\otimes V)|\phi\rangle=0} \langle\phi|(U\otimes V)^\dagger(U\otimes V)\Omega_{opt}(U\otimes V)^\dagger(U\otimes V)|\phi\rangle \tag{S4}$$

$$= \max_{|\phi'\rangle, \langle\psi'|\phi'\rangle=0} \langle\phi'|\Omega'|\phi'\rangle = q'. \tag{S5}$$

So applying the same local rotation to the strategy and the state results in no change in the performance of the strategy. Thus the following simple proof by contradiction holds: assume that there is a better strategy for verifying $|\psi'\rangle$, denoted Ω''. But then the strategy $(U\otimes V)^\dagger\Omega''(U\otimes V)$ must have a better performance for verifying $|\psi\rangle$ than Ω_{opt}, which is a contradiction. Thus Ω' must be the optimal strategy for verifying $|\psi'\rangle$. □

We will now prove Theorem 1 from the main body. However, we first prove a useful lemma - that no optimal strategy can contain the identity measurement (where the verifier always accepts regardless of the tested state). In the following discussion, we denote the projector $\Pi := \mathbb{1} - |\psi\rangle\langle\psi|$. For a strategy Ω where $\Omega|\psi\rangle = |\psi\rangle$, the quantity of interest which determines Δ_ϵ in (S12) is the maximum probability of accepting an orthogonal state $|\psi^\perp\rangle$:

$$q := \|\Pi\Omega\Pi\| = \max_{|\psi^\perp\rangle} \langle\psi^\perp|\Omega|\psi^\perp\rangle. \tag{S6}$$

If a strategy is augmented with an accent or subscript, the parameter q inherits that accent or subscript.

Lemma 4. *Consider an operator $0 \le \Omega \le 1$, $\Omega|\psi\rangle = |\psi\rangle$ of the form $\Omega = (1-\alpha)\Omega_1 + \alpha\mathbb{1}$ for $0 \le \alpha \le 1$. Then $q \ge q_1$.*

Proof. For arbitrary $|\psi^\perp\rangle$ such that $\langle\psi|\psi^\perp\rangle = 0$, $\langle\psi^\perp|\Omega|\psi^\perp\rangle = (1-\alpha)\langle\psi^\perp|\Omega_1|\psi^\perp\rangle + \alpha$. This is maximised by choosing $|\psi^\perp\rangle$ such that $\langle\psi^\perp|\Omega_1|\psi^\perp\rangle = q_1$, giving $q = (1-\alpha)q_1 + \alpha \ge q_1$. □

We are now in a position to prove Theorem 1. Note that the special cases where $|\psi\rangle$ is a product state ($\theta = 0$ or $\frac{\pi}{2}$) or a Bell state ($\theta = \frac{\pi}{4}$) are treated separately.

Theorem 1 (restated). *Any optimal strategy for verifying a state of the form* $|\psi\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ *for* $0 < \theta < \frac{\pi}{2}$, $\theta \neq \frac{\pi}{4}$ *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:*

$$\Omega^{opt} = \frac{2-\sin(2\theta)}{4+\sin(2\theta)} P^+_{ZZ} + \frac{2(1+\sin(2\theta))}{3(4+\sin(2\theta))} \sum_{k=1}^{3} (\mathbb{1} - |\phi_k\rangle\langle\phi_k|), \tag{S7}$$

where the states $|\phi_k\rangle$ *are*

$$|\phi_1\rangle = \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle + \frac{e^{\frac{2\pi i}{3}}}{\sqrt{1+\cot\theta}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle + \frac{e^{\frac{\pi i}{3}}}{\sqrt{1+\cot\theta}}|1\rangle \right), \tag{S8}$$

$$|\phi_2\rangle = \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle + \frac{e^{\frac{4\pi i}{3}}}{\sqrt{1+\cot\theta}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle + \frac{e^{\frac{5\pi i}{3}}}{\sqrt{1+\cot\theta}}|1\rangle \right), \tag{S9}$$

$$|\phi_3\rangle = \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle + \frac{1}{\sqrt{1+\cot\theta}}|1\rangle \right) \otimes \left(\frac{1}{\sqrt{1+\tan\theta}}|0\rangle - \frac{1}{\sqrt{1+\cot\theta}}|1\rangle \right). \tag{S10}$$

The number of measurements needed to verify to within fidelity ϵ *and statistical power* $1-\delta$ *is*

$$n_{opt} \approx (2 + \sin\theta\cos\theta)\epsilon^{-1} \ln \delta^{-1}. \tag{S11}$$

Proof. The strategy Ω can be written as a convex combination of local projectors. We can group the projectors by their action according to two local parties, Alice and Bob, and then it must be expressible as a convex combination of five types of terms, grouped by trace:

$$\Omega = c_1 \sum_i \mu_i (\rho_1^i \otimes \sigma_1^i) + c_2 \sum_j \nu_j (\rho_2^j \otimes \sigma_2^j + \rho_2^{j\perp} \otimes \sigma_2^{j\perp}) + c_3 \sum_k \eta_k (\mathbb{1} - \rho_3^k \otimes \sigma_3^k) + c_4 \sum_l [\zeta_l (\rho_4^l \otimes \mathbb{1}) + \xi_l (\mathbb{1} \otimes \sigma_4^l)] + c_5 \mathbb{1} \otimes \mathbb{1}, \tag{S12}$$

where ρ_i^k and σ_i^k are single-qubit pure states and the subscript denotes the type of term in question. The state $\rho^{j\perp}$ is the density matrix defined by $\mathrm{tr}(\rho^j \rho^{j\perp}) = 0$. Qualitatively, given two local parties Alice and Bob with access to one qubit each, and projectors with outcomes $\{\lambda, \bar{\lambda}\}$, the terms above correspond to the following strategies: (1) Alice and Bob both apply a projective measurement and accept if both outcomes are λ; (2) Alice and Bob both apply a projective measurement and accept if both outcomes agree; (3) Alice and Bob both apply a projective measurement and accept if both outcomes are $\bar{\lambda}$; (4) Alice or Bob applies a projective measurement and accepts on outcome λ, and the other party abstains; and (5) both Alice and Bob accept without applying a measurement.

Given the favourability in scaling with ϵ of the relative entropy with strategies that accept $|\psi\rangle$ with certainty, we enforce this constraint from the outset and then show that a viable strategy can still be constructed. For the general strategy in Eq. S12 to accept $|\psi\rangle$ with certainty, each term in its expansion must accept $|\psi\rangle$ with certainty. However, this is impossible to achieve for some of the terms in the above expansion. In particular, we show that the terms $(\rho \otimes \sigma)$, $(\rho \otimes \mathbb{1})$ and $(\mathbb{1} \otimes \sigma)$ cannot accept $|\psi\rangle$ with certainty, and the form of the term $(\rho \otimes \sigma + \rho^\perp \otimes \sigma^\perp)$ is restricted.

$(\rho \otimes \sigma)$: this term can be reexpressed as a convex combination of projectors onto product states: $\rho \otimes \sigma = \sum_j b_j (|u_j\rangle \otimes |v_j\rangle)(\langle u_j| \otimes \langle v_j|)$, and so this term only accepts $|\psi\rangle$ with certainty if $(\langle u_j| \otimes \langle v_j|)|\psi\rangle = 1, \forall j$. However, for $0 < \theta < \frac{\pi}{2}$ the state $|\psi\rangle$ is entangled and this condition cannot be satisfied.

$(\rho \otimes \mathbb{1})$ or $(\mathbb{1} \otimes \sigma)$: For the term $(\rho \otimes \mathbb{1})$, reexpress ρ in terms of its Pauli expansion: $\rho \otimes \mathbb{1} = \frac{1}{2}(\mathbb{1} + \alpha X + \beta Y + \gamma Z) \otimes \mathbb{1}$, for $-1 \leq \alpha, \beta, \gamma \leq 1$. Then the condition that this term accepts with probability $p = 1$ is

$$\langle\psi| \frac{1}{2}(\mathbb{1} + \alpha X + \beta Y + \gamma Z) \otimes \mathbb{1} |\psi\rangle = 1. \tag{S13}$$

By inserting the definition of $|\psi\rangle$, this becomes $\frac{1}{2}(1 - \gamma\cos(2\theta)) = 1$, which is unsatisfiable for $0 < \theta < \frac{\pi}{2}$. It is readily checkable that an identical condition is derived for the term $\mathbb{1} \otimes \sigma$, given the symmetry of the state $|\psi\rangle$ under swapping.

$(\rho \otimes \sigma + \rho^\perp \otimes \sigma^\perp)$: for this term, we can expand both ρ and σ in terms of Pauli operators:

$$\rho = \frac{1}{2}(\mathbb{1} + \alpha X + \beta Y + \gamma Z); \qquad \rho^\perp = \frac{1}{2}(\mathbb{1} - \alpha X - \beta Y - \gamma Z) \tag{S14}$$

$$\sigma = \frac{1}{2}(\mathbb{1} + \alpha' X + \beta' Y + \gamma' Z); \quad \sigma^\perp = \frac{1}{2}(\mathbb{1} - \alpha' X - \beta' Y - \gamma' Z). \tag{S15}$$

Inserting these expressions and the definition of $|\psi\rangle$ into the condition that $p = 1$ gives the constraint

$$\gamma\gamma' + (\alpha\alpha' - \beta\beta')\sin(2\theta) = 1. \tag{S16}$$

Now, we know from the Cauchy-Schwarz inequality that

$$\gamma\gamma' + (\alpha\alpha' - \beta\beta')\sin(2\theta) \leq \sqrt{\alpha'^2 + \beta'^2 + \gamma'^2}\sqrt{\alpha^2\sin^2(2\theta) + \beta^2\sin^2(2\theta) + \gamma^2} \leq 1, \tag{S17}$$

where the second inequality is derived from the fact that $\{\alpha, \beta, \gamma\}$, $\{\alpha', \beta', \gamma'\}$ are the parameterisation of a pair of density matrices. There are two ways that this inequality can be saturated: (a) $\sin(2\theta) = 1$; (b) $\alpha\alpha' - \beta\beta' = 0$, $\gamma\gamma' = 1$. In all other cases, the inequality is strict. Thus the constraint in Eq. S16 cannot be satisfied in general. Exception (a) corresponds to $\theta = \frac{\pi}{4}$, which is omitted from this proof and treated separately. In exception (b), we have that $\gamma\gamma' = 1$ and so either $\gamma = \gamma' = 1$ or $\gamma = \gamma' = -1$. In both cases we have that

$$\rho \otimes \sigma + \rho^\perp \otimes \sigma^\perp = \left(\frac{\mathbb{1} + Z}{2} \otimes \frac{\mathbb{1} + Z}{2}\right) + \left(\frac{\mathbb{1} - Z}{2} \otimes \frac{\mathbb{1} - Z}{2}\right) = P^+_{ZZ}, \tag{S18}$$

where P^+_{ZZ} is the projector onto the positive eigenspace of ZZ. This is the only possible choice for this particular term that accepts $|\psi\rangle$ with certainty.

We can also make use of Lemma 4 to remove the term $\mathbb{1} \otimes \mathbb{1}$. Given this and the restrictions above from enforcing that $p = 1$, the measurement strategy can be written

$$\Omega = \alpha P^+_{ZZ} + (1 - \alpha)\sum_k \eta_k(\mathbb{1} - \rho_k \otimes \sigma_k), \tag{S19}$$

where $\sum_k \eta_k = 1$ and $0 \leq \alpha \leq 1$.

We'll try to further narrow down the form of this strategy by *averaging*; i.e. by noting that, as $|\psi\rangle$ is an eigenstate of a matrix $M_\zeta \otimes M_{-\zeta}$ where

$$M_\zeta = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\zeta} \end{pmatrix}, \tag{S20}$$

then conjugating the strategy by $M_\zeta \otimes M_{-\zeta}$ and integrating over all possible ζ cannot make the strategy worse; if we consider an averaged strategy $\langle\Omega\rangle$ such that

$$\langle\Omega\rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} d\zeta (M_\zeta \otimes M_{-\zeta})\Omega(M_{-\zeta} \otimes M_\zeta), \tag{S21}$$

then necessarily the performance of $\langle\Omega\rangle$ cannot be worse than that of Ω. To see this, note that the averaging procedure does not affect the probability of accepting the state $|\psi\rangle$. However, for each particular value of ζ the optimisation for the adversary may necessarily lead to different choices for the orthogonal states $|\psi^\perp(\zeta)\rangle$, and so averaging over ζ cannot be better for the adversary than choosing the optimal $|\psi^\perp\rangle$ at $\zeta = 0$.

We can also consider discrete symmetries of the state $|\psi\rangle$. In particular, $|\psi\rangle$ is invariant under both swapping the two qubits, and complex conjugation (with respect to the standard basis); by the same argument, averaging over these symmetries (i.e. by considering $\Omega' = \frac{1}{2}(\Omega + (\mathrm{SWAP})\Omega(\mathrm{SWAP}^\dagger))$ and $\Omega'' = \frac{1}{2}(\Omega + \Omega^*)$) cannot produce strategies inferior to the original Ω. Therefore we can consider a strategy averaged over these families of symmetries of Ω, without any loss in performance.

This averaging process is useful for three reasons. Firstly, it heavily restricts the number of free parameters in Ω requiring optimisation. Secondly, it allows us to be explicit about the general form of Ω. Thirdly, the averaging procedures are distributive over addition; and so we can make the replacement

$$\begin{aligned}\Omega = \alpha P^+_{ZZ} + (1 - \alpha)\sum_k \eta_k(\mathbb{1} - \rho_k \otimes \sigma_k) \to \langle \alpha P^+_{ZZ} + (1 - \alpha)\sum_k \eta_k(\mathbb{1} - \rho_k \otimes \sigma_k)\rangle \\ = \alpha P^+_{ZZ} + (1 - \alpha)\sum_k \eta_k\langle\mathbb{1} - \rho_k \otimes \sigma_k\rangle.\end{aligned} \tag{S22}$$

Note that a single term $\mathbb{1} - \rho_k \otimes \sigma_k$, may, after averaging, be a convex combination of multiple terms of the form $\mathbb{1} - \rho \otimes \sigma$. To proceed, we will use this averaging procedure to show that it suffices to only include a single, post-averaging term of the form $\langle\mathbb{1} - \rho_k \otimes \sigma_k\rangle$ in the strategy Ω, and that the resulting operator can be explicitly decomposed into exactly three measurement settings.

Consider a general operator Ω, expressed as a 4×4 matrix. First, take the discrete symmetries of $|\psi\rangle$. Averaging over complex conjugation in the standard basis implies that the coefficients of $\langle\Omega\rangle$ are real; and averaging over qubit swapping implies that $\langle\Omega\rangle$ is symmetric with respect to swapping of the two qubits. Denote the operator after averaging these discrete symmetries as $\bar{\Omega}$. Then consider averaging over the continuous symmetry of $|\psi\rangle$:

$$\langle\Omega\rangle = \frac{1}{2\pi}\int_{-\pi}^{\pi} d\zeta (M_\zeta \otimes M_{-\zeta})\bar{\Omega}(M_{-\zeta} \otimes M_\zeta) \tag{S23}$$

$$= \frac{1}{2\pi}\int_{-\pi}^{\pi} d\zeta \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\zeta} & 0 & 0 \\ 0 & 0 & e^{-i\zeta} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_{00} & \omega_{01} & \omega_{01} & \omega_{03} \\ \omega_{01} & \omega_{11} & \omega_{12} & \omega_{13} \\ \omega_{01} & \omega_{12} & \omega_{11} & \omega_{13} \\ \omega_{03} & \omega_{13} & \omega_{13} & \omega_{33} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{-i\zeta} & 0 & 0 \\ 0 & 0 & e^{i\zeta} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{S24}$$

$$= \begin{pmatrix} \omega_{00} & 0 & 0 & \omega_{03} \\ 0 & \omega_{11} & 0 & 0 \\ 0 & 0 & \omega_{11} & 0 \\ \omega_{03} & 0 & 0 & \omega_{33} \end{pmatrix}. \tag{S25}$$

Thus after averaging using the above symmetries of $|\psi\rangle$, $\langle\Omega\rangle$ can be written in the standard basis as

$$\langle\Omega\rangle = \begin{pmatrix} a & 0 & 0 & b \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \\ b & 0 & 0 & d \end{pmatrix}, \tag{S26}$$

for $a, b, c, d \in \mathbb{R}$. Enforcing that the strategy accepts $|\psi\rangle$ with certainty yields $\langle\Omega\rangle|\psi\rangle = |\psi\rangle$, or explicitly that

$$\langle\Omega\rangle = \begin{pmatrix} 1 - b\cot\theta & 0 & 0 & b \\ 0 & c & 0 & 0 \\ 0 & 0 & c & 0 \\ b & 0 & 0 & 1 - b\tan\theta \end{pmatrix}. \tag{S27}$$

The eigensystem of this operator is then completely specified; besides $|\psi\rangle$, it has the following eigenvectors:

$$|v_1\rangle = \cos\theta|00\rangle - \sin\theta|11\rangle; \quad |v_2\rangle = |01\rangle; \quad |v_3\rangle = |10\rangle, \tag{S28}$$

with corresponding eigenvalues $\lambda_1 = 1 - b\csc\theta\sec\theta$ and $\lambda_2 = \lambda_3 = c$. The maximum probability of accepting a state orthogonal to $|\psi\rangle$, q, can then be written

$$q = \|\Pi\langle\Omega\rangle\Pi\| = \max\{\lambda_1, \lambda_2\}, \tag{S29}$$

where $\Pi = \mathbb{1} - |\psi\rangle\langle\psi|$. Therefore, any reasoning about q can be reduced to reasoning about the pair (λ_1, λ_2).

Now, we will show that it suffices to only consider a single term of the form $\langle\mathbb{1} - \rho_k \otimes \sigma_k\rangle$ in the decomposition of Ω. We write a strategy of this form as

$$\Omega = \alpha P_{ZZ}^{+} + (1-\alpha)\langle\mathbb{1} - \rho \otimes \sigma\rangle. \tag{S30}$$

For the term $\langle\mathbb{1} - \rho \otimes \sigma\rangle$, we have a constraint on the trace; if we label the eigenvalues for this term as $\lambda_1^{(3)}$ and $\lambda_2^{(3)}$, we have the constraint that $1 + \lambda_1^{(3)} + 2\lambda_2^{(3)} = \mathrm{tr}\langle\mathbb{1} - \rho \otimes \sigma\rangle = 3 \Rightarrow \lambda_2^{(3)} = 1 - \frac{\lambda_1^{(3)}}{2}$. The locus of points satisfying this constraint is plotted in the (λ_1, λ_2) plane as the thick black line in Fig. S1. Moreover, we will show that a single term of this form can achieve any valid choice of $\lambda_1^{(3)}$ on this locus (which we defer until we have an explicit parameterisation of terms of this type; see Eq. S42, below).

However, we also have an additional constraint derived from insisting that the strategy remains local. For example, the point $(1, 0)$ in the (λ_1, λ_2) plane represents the strategy $\Omega = \mathbb{1} - |v_1\rangle\langle v_1|$, which corresponds to the strategy where the verifier projects onto $|v_1\rangle$ and accepts if the outcome is not $|v_1\rangle$. But this type of measurement is operationally forbidden as $|v_1\rangle$ is entangled.

It can be readily checked that, for an arbitrary θ, it is not possible to cover the full locus in the range $0 \leq \lambda_1 \leq 1$ with a separable strategy; instead, there is a fixed lower bound on $\lambda_1^{(3)}$. To see this, write

$$\langle\mathbb{1} - \rho \otimes \sigma\rangle = |\psi\rangle\langle\psi| + \lambda_1^{(3)}|v_1\rangle\langle v_1| + \frac{2 - \lambda_1^{(3)}}{2}(|v_2\rangle\langle v_2| + |v_3\rangle\langle v_3|). \tag{S31}$$

Then, taking just the $\langle \rho \otimes \sigma \rangle$ part and expressing as a matrix in the computational basis gives

$$\langle \rho \otimes \sigma \rangle = \begin{pmatrix} (1-\lambda_1^{(3)})\cos^2\theta & 0 & 0 & (\lambda_1^{(3)}-1)\cos\theta\sin\theta \\ 0 & \frac{\lambda_1^{(3)}}{2} & 0 & 0 \\ 0 & 0 & \frac{\lambda_1^{(3)}}{2} & 0 \\ (\lambda_1^{(3)}-1)\cos\theta\sin\theta & 0 & 0 & (1-\lambda_1^{(3)})\sin^2\theta \end{pmatrix}. \tag{S32}$$

To enforce separability it is necessary and sufficient to check positivity under partial transposition, yielding the constraint $\lambda_1^{(3)} - (1-\lambda_1^{(3)})\sin(2\theta) \geq 0$. Simple rearrangement gives a lower bound that must be satisfied for the strategy to remain separable:

$$\lambda_1^{(3)} \geq \frac{\sin(2\theta)}{1+\sin(2\theta)} := \lambda_{LB}. \tag{S33}$$

This additional locality constraint rules out any point on the black line to the left of the red point in Fig. S1. The term P_{ZZ}^{+} has parameters $\lambda_1^{ZZ} = 1$, $\lambda_2^{ZZ} = 0$ and so represents a single point in the (λ_1, λ_2) plane. Thus the parameters (λ_1, λ_2) for the full strategy Ω must be represented by a point in the convex hull of the single point representing the P_{ZZ}^{+} term and the locus of points representing the trace 3 part - i.e. in the unshaded region in Fig. S1.

We now show that a strategy that includes more trace 3 terms cannot improve on the performance of the strategy above. Write this expanded strategy as

$$\Omega' = \alpha P_{ZZ}^{+} + (1-\alpha)\langle \sum_k \eta_k (\mathbb{1} - \rho_k \otimes \sigma_k) \rangle, \tag{S34}$$

for $\sum_k \eta_k = 1$. Firstly, we note again that the averaging operations (SWAP, conjugation via M_ζ and complex conjugation in the standard basis) are distributive over addition and so we can make the replacement

$$\Omega' = \alpha P_{ZZ}^{+} + (1-\alpha) \sum_k \eta_k \langle \mathbb{1} - \rho_k \otimes \sigma_k \rangle. \tag{S35}$$

Write the composite term $\sum_k \eta_k \langle \mathbb{1} - \rho_k \otimes \sigma_k \rangle := \Omega_{\text{comp}}$, with parameters λ_1^{comp} and λ_2^{comp}. Note that each term in Ω_{comp} satisfies both the constraint from the trace and the constraint from PPT in S33, and hence so does Ω_{comp}. Now, each operator in this term shares the same eigenbasis (namely, the set of states $\{|v_i\rangle\}$ in S28). Thus we know that $\lambda_1^{\text{comp}} = \sum_k \eta_k \lambda_{1,k}$, and likewise for λ_2^{comp}; i.e. the strategy parameters for this composite term are just a convex combination of those for its constituent parts. A term Ω_{comp} is then specified in the (λ_1, λ_2) plane by a point $\mathcal{P}_{\text{comp}} = (\lambda_1^{\text{comp}}, \lambda_2^{\text{comp}}) \in \text{Conv}(\lambda_{1,k}, \lambda_{2,k})$ (i.e. the point $\mathcal{P}_{\text{comp}}$ must lie on the thick black line bounding the unshaded region in Fig. S1).

Thus we know that $\text{Conv}(\Omega') \subseteq \text{Conv}(\Omega)$, and so any strategy writeable in the form S34 can be replaced by a strategy of the form S30 with identical parameters (λ_1, λ_2), and hence identical performance. Thus, we need only consider strategies of the form

$$\Omega = \alpha P_{ZZ}^{+} + (1-\alpha)\langle \mathbb{1} - \rho \otimes \sigma \rangle. \tag{S36}$$

We can now be explicit about the form of the above strategy. For Ω to accept $|\psi\rangle$ with certainty, $\rho \otimes \sigma$ must annihilate $|\psi\rangle$ and so we make the replacement $\rho \otimes \sigma = |\tau\rangle\langle\tau|$, where $|\tau\rangle$ is the most general pure product state that annihilates $|\psi\rangle$. To be explicit about the form of the state $|\tau\rangle$, write a general two-qubit separable state as

$$|\tau\rangle = (\cos\phi|0\rangle + e^{i\eta}\sin\phi|1\rangle) \otimes (\cos\xi|0\rangle + e^{i\zeta}\sin\xi|1\rangle), \tag{S37}$$

where we take $0 \leq \phi, \xi \leq \frac{\pi}{2}$, without loss of generality. The constraint that this state annihilates $|\psi\rangle = \sin\theta|00\rangle + \cos\theta|11\rangle$ is

$$\cos\phi\cos\xi\sin\theta + e^{-i(\eta+\zeta)}\sin\phi\sin\xi\cos\theta = 0. \tag{S38}$$

If either $\phi = 0$ or $\xi = 0$, then $\cos\phi\cos\xi\sin\theta = 0$ implying that $\xi = \frac{\pi}{2}$ or $\phi = \frac{\pi}{2}$, respectively. This yields the annihilating states $|\tau\rangle = |01\rangle$ and $|\tau\rangle = |10\rangle$, respectively. If $\phi, \xi \neq 0$ then from the imaginary part of Eq. S38 we find that $e^{-i(\eta+\zeta)} = -1$. Then we can rearrange to give

$$\tan\phi\tan\xi = \tan\theta. \tag{S39}$$

Using this constraint and the identities

$$\cos\xi = \frac{1}{\sqrt{1+\tan^2\xi}}; \quad \sin\xi = \frac{\tan\xi}{\sqrt{1+\tan^2\xi}}, \tag{S40}$$

we can eliminate ξ to yield

$$|\tau\rangle = (\cos\phi|0\rangle + e^{i\eta}\sin\phi|1\rangle) \otimes \left(\frac{\tan\phi}{\sqrt{\tan^2\phi+\tan^2\theta}}|0\rangle - \frac{e^{-i\eta}\tan\theta}{\sqrt{\tan^2\phi+\tan^2\theta}}|1\rangle\right). \tag{S41}$$

Note that, for $0 < \theta < \frac{\pi}{2}$, taking the limits $\phi \to 0$ and $\phi \to \frac{\pi}{2}$ we recover the cases $|\tau\rangle = |01\rangle$ and $|\tau\rangle = |10\rangle$, up to irrelevant global phases. Thus we can proceed without loss of generality by assuming that $\rho \otimes \sigma = |\tau\rangle\langle\tau|$, where $|\tau\rangle$ is given by Eq. S41. Averaging over the symmetries of $|\psi\rangle$ outlined above then yields the following expression:

$$\langle\rho\otimes\sigma\rangle = \frac{1}{\tan^2\phi+\tan^2\theta}\begin{pmatrix} \sin^2\phi & 0 & 0 & -\sin^2\phi\tan\theta \\ 0 & \frac{1}{2}\left(\cos^2\phi\tan^2\theta+\sin^2\phi\tan^2\phi\right) & 0 & 0 \\ 0 & 0 & \frac{1}{2}\left(\cos^2\phi\tan^2\theta+\sin^2\phi\tan^2\phi\right) & 0 \\ -\sin^2\phi\tan\theta & 0 & 0 & \sin^2\phi\tan^2\theta \end{pmatrix}. \tag{S42}$$

Given this explicit parameterisation we can extract the eigenvalue $\lambda_1^{(3)}$:

$$\lambda_1^{(3)} = 1 - \frac{\sec^2\theta\sin^2\phi}{\tan^2\theta+\tan^2\phi}. \tag{S43}$$

It can be shown by simple differentiation w.r.t. ϕ that, for fixed θ, this expression has a minimum at $\lambda_1^{(3)} = \lambda_{LB}$. Also, this expression is a continuous function of ϕ and therefore can take any value up to its maximum (namely, 1). Hence a single trace 3 term is enough to achieve any point in the allowable convex hull in Fig. S1. For convenience we will denote $\tan^2\phi = P$, $\tan^2\theta = T$ for $0 \le P \le \infty$, $0 < T < \infty$. The explicit form for the whole strategy is then

$$\Omega = \frac{1}{(1+P)(P+T)}\begin{pmatrix} T+P(P+T+\alpha) & 0 & 0 & (1-\alpha)P\sqrt{T} \\ 0 & \frac{1}{2}(1-\alpha)(T+2P+P^2+2PT) & 0 & 0 \\ 0 & 0 & \frac{1}{2}(1-\alpha)(T+2P+P^2+2PT) & 0 \\ (1-\alpha)P\sqrt{T} & 0 & 0 & T+P(1+P+\alpha T) \end{pmatrix}. \tag{S44}$$

We now optimise over the two remaining free parameters, $\{\alpha, \phi\}$ (or alternatively, $\{\alpha, P\}$) for fixed θ (or fixed T). We have shown that it suffices to consider the eigenvalues λ_1 and λ_2, given in this case by the expressions

$$\lambda_1(\alpha,P,T) = 1 - \frac{P(1-\alpha)(1+T)}{(1+P)(P+T)}; \quad \lambda_2(\alpha,P,T) = (1-\alpha)\left[1 - \frac{T+P^2}{2(1+P)(P+T)}\right]. \tag{S45}$$

The parameter q is given by the maximum of these two eigenvalues. Note that, if $P = 0$, the expression $\lambda_1(\alpha, 0, T) = 1$ which implies that the adversary can pick a state that the verifier always accepts, and hence the strategy fails. Likewise, taking the limit $\lim_{P\to\infty}\lambda_1(\alpha,P,T) = 1$. Thus we must restrict to the range $0 < P < \infty$ to construct a viable strategy for the verifier. The quantity q is minimised for fixed T when the derivatives with respect to P and α vanish. First, we calculate the derivatives w.r.t. α:

$$\frac{\partial\lambda_1}{\partial\alpha} = \frac{P(1+T)}{(1+P)(P+T)}; \quad \frac{\partial\lambda_2}{\partial\alpha} = \frac{-(2P+P^2+T+2PT)}{2(1+P)(P+T)}. \tag{S46}$$

Given that $P > 0$ and $T > 0$, we have that for any choice of T, $\partial_\alpha\lambda_1 > 0$ and $\partial_\alpha\lambda_2 < 0$. Thus, one of three cases can occur: (a) for a given choice of T and P, the lines given by λ_1 and λ_2 intersect in the range $0 \le \alpha \le 1$ and hence there is a valid α such that q is minimised when $\lambda_1 = \lambda_2$; (b) for a given choice of T and P, $\lambda_1 > \lambda_2$ in the range $0 \le \alpha \le 1$ and hence q is minimised when $\alpha = 0$; (c) for a given choice of T and P, $\lambda_1 < \lambda_2$ in the range $0 \le \alpha \le 1$ and hence q is minimised when $\alpha = 1$. However, we note that this final case cannot occur; it suffices to check that $\lambda_1(\alpha = 1) > \lambda_2(\alpha = 1)$, and from the expressions in (S45) we have that $\lambda_1(\alpha = 1) = 1$ and $\lambda_2(\alpha = 1) = 0$. As a visual aid for the remaining two cases, see Fig. S2. In case (a),

$$q = \lambda_1 = \lambda_2 = \frac{1}{2} + \frac{1}{2}\left(\frac{T+P^2}{T+P^2+4P(1+T)}\right). \tag{S47}$$

In case (b), we have that

$$q = \lambda_1(0, P, T) = \frac{T + P^2}{(1 + P)(P + T)}. \tag{S48}$$

We must also minimise w.r.t. ϕ; however, we can safely minimise w.r.t. P as $\partial_\phi P > 0$ (unless $\phi = 0$, but in this case $q = 1$ and the strategy fails). In case (b), we have

$$\frac{\partial q}{\partial P} = \frac{(P^2 - T)(1 + T)}{(1 + P)^2(P + T)^2}. \tag{S49}$$

In this case, consider the two points implicitly defined by the constraint $\lambda_1(0, P, T) = \lambda_2(0, P, T)$ (drawn as the black points in Fig. S2). Denote these points $f^{\pm}(T)$. It can be readily checked that in case (b), $\partial_P q < 0$ for any $q < f^-(T)$, and $\partial_P q > 0$ for any $q > f^+(T)$. Thus the minimum w.r.t P must occur when $\lambda_1(0, P, T) = \lambda_2(0, P, T)$ and hence we can restrict our attention to case (a) (note Fig. S2). In this case, $\partial_P q$ becomes

$$\frac{\partial q}{\partial P} = \frac{-2(1 + T)(T - P^2)}{[T + 4PT + P(4 + P)]^2} = 0, \tag{S50}$$

which implies that $P = \sqrt{T}$. Substituting in the optimal choices for the parameters $\{\alpha, P\}$ and reexpressing solely in terms of θ gives the optimal strategy

$$\Omega^{opt} = \frac{2 - \sin(2\theta)}{4 + \sin(2\theta)} P^+_{ZZ} + \frac{2(1 + \sin(2\theta))}{4 + \sin(2\theta)} \Omega_3^{opt}, \tag{S51}$$

where Ω_3^{opt} is given by

$$\Omega_3^{opt} = \mathbb{1} - \frac{1}{(1 + t)^2} \begin{pmatrix} 1 & 0 & 0 & -t \\ 0 & t & 0 & 0 \\ 0 & 0 & t & 0 \\ -t & 0 & 0 & t^2 \end{pmatrix}, \quad t = \tan\theta. \tag{S52}$$

This strategy accepts an orthogonal state with probability

$$q_{opt} = \frac{2 + \sin(2\theta)}{4 + \sin(2\theta)}, \tag{S53}$$

implying that the number of measurements needed to verify to within accuracy ϵ and with statistical power $1 - \delta$ under this test is

$$n_{opt} = \frac{\ln \delta^{-1}}{\ln((1 - \Delta_\epsilon)^{-1})} = \frac{\ln \delta^{-1}}{\ln((1 - \epsilon(1 - q^{opt}))^{-1})} \approx (2 + \sin\theta\cos\theta)\epsilon^{-1} \ln \delta^{-1}. \tag{S54}$$

The final step is to show that the operator Ω_3^{opt} can be decomposed into a small set of locally implementable, projective measurements. We can do so with a strategy involving only three terms:

$$\Omega_3^{opt} = \frac{1}{3} \left[\sum_{k=1}^{3} (\mathbb{1} - |\phi_k\rangle\langle\phi_k|) \right], \tag{S55}$$

where the set of separable states $\{|\phi_k\rangle\}$ are the following:

$$|\phi_1\rangle = \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle + \frac{e^{\frac{2\pi i}{3}}}{\sqrt{1 + \cot\theta}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle + \frac{e^{\frac{\pi i}{3}}}{\sqrt{1 + \cot\theta}} |1\rangle \right), \tag{S56}$$

$$|\phi_2\rangle = \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle + \frac{e^{\frac{4\pi i}{3}}}{\sqrt{1 + \cot\theta}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle + \frac{e^{\frac{5\pi i}{3}}}{\sqrt{1 + \cot\theta}} |1\rangle \right), \tag{S57}$$

$$|\phi_3\rangle = \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle + \frac{1}{\sqrt{1 + \cot\theta}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{1 + \tan\theta}} |0\rangle - \frac{1}{\sqrt{1 + \cot\theta}} |1\rangle \right), \tag{S58}$$

which gives a strategy of the required form. □

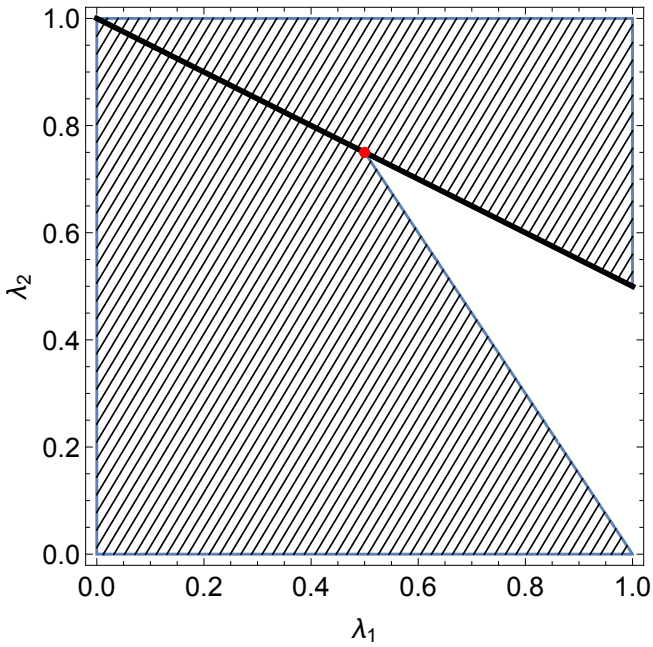

FIG. S1. Shaded region: unreachable parameters given a strategy Ω that is both local and of the form $\Omega = \alpha P^+_{ZZ} + (1-\alpha)\Omega_3$, where Ω_3 is the trace 3 part. Here, $\theta = \frac{\pi}{8}$.

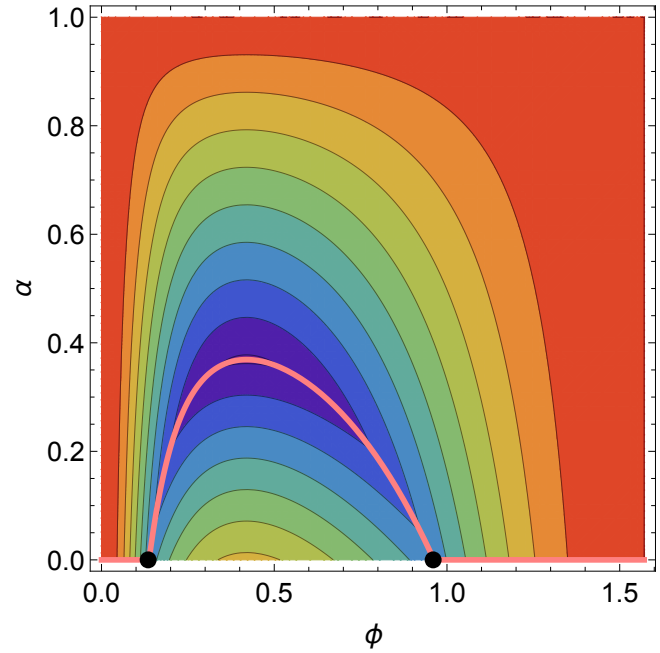

FIG. S2. A contour map of the function $q(\alpha,\phi) = \max\{\lambda_1(\alpha,\phi), \lambda_2(\alpha,\phi)\}$ for $\theta = \frac{\pi}{8}$, where the pair (λ_1, λ_2) are given in S45. The pink curve denotes the minimum w.r.t α given fixed ϕ. Above the curve, $\lambda_1 > \lambda_2$; below, $\lambda_1 < \lambda_2$.

We now briefly treat the special cases that were omitted from the above proof: $\theta = 0, \frac{\pi}{4}, \frac{\pi}{2}$.
$\theta = 0, \theta = \frac{\pi}{2}$: In these cases, the state $|\psi\rangle = |00\rangle$ or $|\psi\rangle = |11\rangle$. Then the globally optimal strategy, just projecting onto $|\psi\rangle$, is an allowed local measurement. Thus in these cases the optimal strategy is to just apply the projector $|00\rangle\langle 00|$ or $|11\rangle\langle 11|$. Given this strategy we have that $p = 1$ and $q = 0$, giving a scaling of the number of measurements required as

$$n_{opt} \approx \epsilon^{-1} \ln \delta^{-1}. \tag{S59}$$

$\theta = \frac{\pi}{4}$: This case is treated explicitly in the main body. The optimal strategy is to perform the Pauli measurements XX, $-YY$ and ZZ with equal weight; i.e.

$$\Omega = \frac{1}{3}(P^+_{XX} + P^+_{-YY} + P^+_{ZZ}), \tag{S60}$$

where P^+_M is the projector onto the positive eigensubspace of the operator M. In this case, the number of measurements required is

$$n_{opt} \approx \frac{3}{2}\epsilon^{-1} \ln \delta^{-1}. \tag{S61}$$

Appendix D: Stabilizer states

Assume now that $|\psi\rangle$ is a stabilizer state of N qubits, namely that there exist a generating set of N commuting Pauli operators $M_1, \ldots, M_N$ on N qubits such that $M_i|\psi\rangle = |\psi\rangle$ for all i. We will describe below a strategy constructed from only stabilizer measurements that accepts $|\psi\rangle$ with certainty, and hence achieves the same asymptotic scaling in the number of required measurements with respect to ϵ as the two-qubit case above. However, we do not rule out that there may be non-stabilizer strategies that give a small constant factor improvement over the strategy defined here.

Theorem 5. *Write a stabilizer state $|\psi\rangle$ and strategy $\Omega = \sum_{j=1}^{K} \mu_j P_j$, where the set $\{P_j\}$ are the projectors onto the positive eigenspace of K linearly independent stabilizers of $|\psi\rangle$, for $K \leq 2^N - 1$. Then the optimal choice of the*

parameter K and weights μ_j are $K = 2^N - 1$; $\mu_j = \frac{1}{2^N-1}$ for all j. The number of measurements needed to verify to within fidelity ϵ and statistical power $1-\delta$ is then

$$n_{opt}^{stab} \approx \frac{2^N - 1}{2^{(N-1)}} \epsilon^{-1} \ln \frac{1}{\delta}. \tag{S1}$$

Proof. Recall that as the verifier accepts $|\psi\rangle$ with certainty, we are concerned with the optimisation of Δ_ϵ, which can be written as

$$\Delta_\epsilon = \max_{\Omega} \min_{|\psi^\perp\rangle} \epsilon(1 - \langle\psi^\perp|\Omega|\psi^\perp\rangle) \tag{S2}$$

$$= \epsilon(1 - \min_{\Omega} \max_{|\psi^\perp\rangle} \langle\psi^\perp|\Omega|\psi^\perp\rangle), \tag{S3}$$

where the maximisation is over positive matrices Ω such that $\Omega|\psi\rangle = |\psi\rangle$.

Now consider Ω written as a matrix in the basis $\{|\psi\rangle, |\psi_j^\perp\rangle\}$, $j = 1 \ldots (2^N - 1)$ where the states $|\psi_j^\perp\rangle$ are mutually orthogonal and all orthogonal to $|\psi\rangle$. Given that $\Omega|\psi\rangle = |\psi\rangle$, we know that $\langle\psi_j^\perp|\Omega|\psi\rangle = 0\ \forall j$. Then in this basis Ω can be written

$$\Omega = \begin{pmatrix} 1 & \mathbf{0}^\top \\ \mathbf{0} & \mathbf{M} \end{pmatrix}, \tag{S4}$$

where $\mathbf{0}$ is the $(2^N - 1)$-dimensional zero vector and $\mathbf{M}$ is a $(2^N - 1) \times (2^N - 1)$ Hermitian matrix. Then Ω must be writable as $\Omega = |\psi\rangle\langle\psi| + \sum_{j=1}^{2^N-1} \nu_j |\phi_j\rangle\langle\phi_j|$, where $\sum_j \nu_j |\phi_j\rangle\langle\phi_j|$ is the spectral decomposition of $\mathbf{M}$. Given this decomposition, the optimisation for the adversary is straightforward – pick $|\psi^\perp\rangle$ to be the eigenstate in the decomposition of $\mathbf{M}$ with largest eigenvalue: $|\psi^\perp\rangle = |\phi_{max}\rangle$ where $\nu_{max} = \max_j \nu_j$. Then

$$\Delta_\epsilon = \epsilon(1 - \min_{\Omega} \langle\phi_{max}|\Omega|\phi_{max}\rangle) = \epsilon(1 - \min_{\Omega} \nu_{max}). \tag{S5}$$

Given this choice by the adversary, the verifier is then forced to set the strategy such that all the eigenvalues of $\mathbf{M}$ are equal; i.e. that $\mathbf{M} = a\mathbb{1}$ for some constant a. To see this, consider an alternative strategy where the eigenvalues ν_j are not equal. Now, consider rewriting Ω in terms of stabilizers of $|\psi\rangle$. For any stabilizer (i.e. tensor product of Paulis, perhaps with an overall phase) M over N qubits, the projector onto the positive eigensubspace has $\mathrm{tr}(P_M^+) = 2^{N-1}$. Given that Ω is built from a convex combination of these projectors, and recalling from Lemma 4 that Ω does not contain an identity term, we also know that $\mathrm{tr}(\Omega) = 2^{N-1}$. However, we have also expanded Ω as $\Omega = |\psi\rangle\langle\psi| + \sum_j \nu_j |\phi_j\rangle\langle\phi_j|$, and so

$$\mathrm{tr}(\Omega) = 1 + \sum_j \nu_j = 2^{N-1}. \tag{S6}$$

Then, it is straightforward to see that decreasing any eigenvalue below a must result in an increase in at least one other eigenvalue in order to maintain this equality, and hence would increase the value of ν_{max}. Thus the optimal choice for the verifier is to set $\Omega = |\psi\rangle\langle\psi| + a\mathbb{1}^\perp$, where $\mathbb{1}^\perp$ is the identity matrix on the subspace orthogonal to $|\psi\rangle$. Taking the trace of this expression gives

$$\mathrm{tr}[|\psi\rangle\langle\psi| + a\mathbb{1}^\perp] = 1 + (2^N - 1)a = 2^{N-1}. \tag{S7}$$

This can be rearranged for a and then substituted into the expression for Δ_ϵ, which gives

$$\Delta_\epsilon = \frac{2^{(N-1)}}{2^N - 1}\epsilon, \tag{S8}$$

or that the number of stabilizer measurements required to verify $|\psi\rangle$ is bounded below by

$$n_{opt}^{stab} \approx \frac{2^N - 1}{2^{(N-1)}} \epsilon^{-1} \ln \delta^{-1}. \tag{S9}$$

The optimal $\Omega = |\psi\rangle\langle\psi| + \frac{2^{(N-1)}-1}{2^N-1}\mathbb{1}^\perp$ and the optimal scaling above can be achieved by decomposing Ω into a strategy involving a maximal set (excluding the identity) of $2^N - 1$ linearly independent stabilizers, all with equal weight. To see this note that for a stabilizer group of a state $|\psi\rangle$ of N qubits, there are 2^N stabilizers independent

under multiplication (including the identity element). Denote these stabilizers $\{M_i, i = 1 \dots 2^N\}$. Then, we make use of the fact that [S24]

$$\frac{1}{2^N} \sum_{i=1}^{2^N} M_i = |\psi\rangle\langle\psi|. \tag{S10}$$

Explicitly extracting the identity element gives

$$\sum_{i=1}^{2^N-1} M_i = 2^N |\psi\rangle\langle\psi| - \mathbb{1}. \tag{S11}$$

Now, each stabilizer (for any N) is a two outcome measurement and so we can make use of the fact that M_i can be written in terms of the projector onto the positive eigenspace of M_i, denoted P_i^+, as $M_i = 2P_i^+ - \mathbb{1}$. Substituting in this expression and rearranging gives

$$\sum_{i=1}^{2^N-1} P_i^+ = 2^{(N-1)} |\psi\rangle\langle\psi| + (2^{(N-1)} - 1)\mathbb{1}. \tag{S12}$$

Then normalising this expression over $2^N - 1$ stabilizers yields

$$\begin{aligned} \frac{1}{2^N-1} \sum_{i=1}^{2^N-1} P_i^+ &= \frac{2^{(N-1)}}{2^N-1} |\psi\rangle\langle\psi| + \frac{2^{(N-1)}-1}{2^N-1} \mathbb{1} \\ &= \frac{2^{(N-1)} + 2^{(N-1)} - 1}{2^N-1} |\psi\rangle\langle\psi| + \frac{2^{(N-1)}-1}{2^N-1} \mathbb{1}^\perp \\ &= |\psi\rangle\langle\psi| + \frac{2^{(N-1)}-1}{2^N-1} \mathbb{1}^\perp = \Omega, \end{aligned} \tag{S13}$$

where $\mathbb{1}^\perp$ is the identity matrix on the subspace orthogonal to $|\psi\rangle$, as required. □

Note that for growing N, the quantity n_{opt}^{stab} given in Eq. S9 is bounded above by $2\epsilon^{-1} \ln \delta^{-1}$, which does not depend on N, and implies that this stabilizer strategy requires at most a factor of two more measurements than the optimal non-local verification strategy (just projecting onto $|\psi\rangle$).

One could also consider a reduced strategy that involves measuring fewer stabilizers. However, given a state of N qubits and a set of k stabilizers, the dimension of the subspace stabilized by this set is at least 2^{N-k}. Thus for any choice of $k < N$, there must always exist at least one state $|\psi^\perp\rangle$ orthogonal to $|\psi\rangle$ that is stabilized by every stabilizer in the set. Then, the adversary can construct a σ that always accepts, implying that the verifier has no discriminatory power between $|\psi\rangle$ and σ and thus the strategy fails. Consider instead constructing a strategy from the N stabilizer generators of $|\psi\rangle$, with corresponding projectors $\{P_j^{s.g.}\}$. Then, $\Omega = \sum_j \mu_j P_j^{s.g.}$. The set of projectors $\{P_j^{s.g.}\}$ commute and so share a common eigenbasis, denoted $\{|\lambda_j\rangle\}$. To optimise this strategy over the weights μ_j, we first need the following lemma:

Lemma 6. *Write the unique sets of $N-1$ independent stabilizer generators of $|\psi\rangle$, $S_k = \{M_j, j = 1 \dots N\} \setminus M_k$, $k = 1 \dots N$. Then for each S_k, there exists a unique $|\lambda_k\rangle$, $\langle\lambda_k|\psi\rangle = 0$, stabilized by all the elements of this set.*

Proof. Each set S_k stabilizes a space of dimension two, and so a $|\lambda_k\rangle$ of the required form exists. To show uniqueness (up to a constant), assume the converse: that there exist two sets S_k and S_ℓ such that $M_k|\lambda_k\rangle = |\lambda_k\rangle$ for all $M_k \in S_k$, and $M_\ell|\lambda_k\rangle = |\lambda_k\rangle$ for all $M_\ell \in S_\ell$. But the set of all stabilizer generators is $S_k \cup S_\ell$, which then stabilizes $|\lambda_k\rangle$; which is a contradiction, as the full set of stabilizer generators uniquely stabilizes $|\psi\rangle$. □

We can now derive the optimal stabilizer generator strategy.

Theorem 7. *For a stabilizer state $|\psi\rangle$ and strategy $\Omega = \sum_{j=1}^N \mu_j P_j^{s.g.}$, where the set $\{P_j^{s.g.}\}$ are the projectors onto the positive eigenspace of the stabilizer generators of $|\psi\rangle$, the optimal choice of the weights μ_j is $\mu_j = \frac{1}{N}$, for all j. The number of measurements needed to verify to within fidelity ϵ and statistical power $1-\delta$ is then*

$$n_{opt}^{s.g.} \approx \frac{N}{\epsilon} \ln \frac{1}{\delta}. \tag{S14}$$

Proof. If we write a state orthogonal to $|\psi\rangle$ in the stabilizer eigenbasis as $|\psi^\perp\rangle = \sum_k \alpha_k |\lambda_k\rangle$, we have that

$$\begin{aligned}\langle\psi^\perp|\Omega|\psi^\perp\rangle &= \sum_{k,m=1}^{2^N}\sum_{j=1}^{N} \bar{\alpha}_k \alpha_m \mu_j \langle\lambda_k|P_j^{s.g.}|\lambda_m\rangle \\ &= \sum_{k,m=1}^{2^N}\sum_{j=1}^{N} \bar{\alpha}_k \alpha_m \mu_j \delta_{km}\epsilon_{jk} \\ &= \sum_{k=1}^{2^N}\sum_{j=1}^{N} |\alpha_k|^2 \mu_j \epsilon_{jk} \coloneqq \sum_{k=1}^{2^N} |\alpha_k|^2 E_k, \end{aligned} \tag{S15}$$

where $\epsilon_{jk} = 1$ if $P_j|\lambda_k\rangle = |\lambda_k\rangle$ and zero otherwise. This quantity is the *parity-check matrix* for the set of stabilizers $\{P_j^{s.g.}\}$. The quantity of interest with respect to verification is

$$q = \min_{\Omega}\max_{|\psi^\perp\rangle} \langle\psi^\perp|\Omega|\psi^\perp\rangle = \min_{\mu_j}\max_{\alpha_k} \sum_{j,k} |\alpha_k|^2 \mu_j \epsilon_{jk}. \tag{S16}$$

Lemma 6 gives that there is a set of orthogonal basis states $|\lambda_{\tilde{k}}\rangle$, $\tilde{k} \in I$ for $|I| = N$, stabilized by exactly $N-1$ generators; thus the quantity $\epsilon_{j\tilde{k}} = 1$ for all j, unless $j = \tilde{k}$. For these terms, the summation over j is

$$E_{\tilde{k}} = \sum_j \mu_j \epsilon_{j\tilde{k}} = 1 - \mu_{\tilde{k}}, \tag{S17}$$

using the fact that $\sum_j \mu_j = 1$. Now, each element of E_k for $k \notin I$ is a summation of at most $N-2$ terms, μ_j. Thus there always exists another element $E_{\tilde{k}}$ for $\tilde{k} \in I$ that is at least as large; and so it is never detrimental to the adversary to shift any amplitude on the basis state labelled by k to the basis state labelled by $\tilde{k}$. Thus the optimal choice for the adversary's state is $|\psi^\perp\rangle \in \text{span}\{|\lambda_{\tilde{k}}\rangle : \tilde{k} \in I\}$. Given this choice by the adversary, we have that

$$q = \min_{\mu_{\tilde{k}}}\max_{\alpha_{\tilde{k}}} \sum_{\tilde{k}} |\alpha_{\tilde{k}}|^2 (1 - \mu_{\tilde{k}}) = \min_{\mu_{\tilde{k}}}\max_{\tilde{k}} (1 - \mu_{\tilde{k}}). \tag{S18}$$

It is straightforward to see that the optimal choice for the verifier is to have $\mu_{\tilde{k}} = \frac{1}{N}$, for all $\tilde{k}$; then $\Omega = \frac{1}{N}\sum P_j^{s.g.}$. Thus

$$q = 1 - \frac{1}{N} \Rightarrow n_{opt}^{s.g.} \approx \frac{N}{\epsilon}\ln\frac{1}{\delta}. \tag{S19}$$

□

Clearly, this scaling is much poorer in N than in the case where the full set of $2^N - 1$ linearly independent stabilizers are allowed; indicating a trade-off between the total number of required measurements and the accessible number of measurement settings, in this case.

Appendix E: Concentration inequalities and the relative entropy

In a binary hypothesis test between hypotheses H_0 and H_1, the Type I and Type II errors are, respectively,

$$\text{Type I}: \quad \Pr[\text{Guess } H_1|H_0] \tag{S1}$$
$$\text{Type II}: \quad \Pr[\text{Guess } H_0|H_1]. \tag{S2}$$

In general, in designing an effective hypothesis test there will be a trade-off between the relative magnitude of these types of error; they cannot be arbitrarily decreased simultaneously. In an *asymmetric* hypothesis test, the goal is to minimise one of these errors given a fixed upper bound on the other. In this addendum, we prove the following proposition in the context of asymmetric hypothesis testing:

Proposition 8. *Any strategy Ω that: (a) accepts $|\psi\rangle$ with certainty, $p \coloneqq \text{tr}(\Omega|\psi\rangle\langle\psi|) = 1$; and (b) does not accept σ with certainty ($\Delta_\epsilon > 0$) requires asymptotically fewer measurements in infidelity ϵ to distinguish these states to within a fixed Type II error than the best protocol based on a strategy Ω' where $\text{tr}(\Omega'|\psi\rangle\langle\psi|) < 1$.*

We have inherited notation regarding verification strategies from Appendix A. Here, hypothesis H_0 corresponds to accepting the target $|\psi\rangle$, and hypothesis H_1 corresponds to accepting the alternative (that the output was far from $|\psi\rangle$). Proposition 8 states that, in a framework where we attempt to verify $|\psi\rangle$ by repeatedly making two-outcome measurements picked from some set, asymptotically it is always beneficial to use measurements that accept $|\psi\rangle$ with certainty. In this case, each measurement is a Bernoulli trial with some acceptance probability. An example of a protocol which would *not* satisfy this property would be estimating the probability of violating a Bell inequality for a maximally entangled 2-qubit state $|\psi\rangle$.

In general, the optimum asymptotic rate at which the Type II error can be minimised in an asymmetric hypothesis test is given by the *Chernoff-Stein lemma*:

Theorem 9 (Cover and Thomas [S25], Theorem 11.8.3.)**.** *Let $X_1, X_2 \dots X_n$ be drawn i.i.d. from a probability mass function Q. Then consider the hypothesis test between alternatives H_0: $Q = P_0$ and H_1: $Q = P_1$. Let A_n be an acceptance region for the null hypothesis H_0; i.e. it is a set consisting of all possible strings of outcomes with which the conclusion H_0 is drawn. Denote Type I and Type II errors after n samples as α_n^* and β_n^*, respectively. Then for some constraint parameter $0 < \chi < \frac{1}{2}$, define*

$$\delta_n^\chi = \min_{\substack{A_n \\ \alpha_n^* < \chi}} \beta_n^*.$$

Then asymptotically

$$\lim_{n\to\infty} \frac{1}{n} \log \delta_n^\chi = -D(P_0 \,\|P_1),$$

where $D(P_0\|P_1)$ is the relative entropy between probability distributions P_0 and P_1.

For clarity we drop the sub- and superscript $\delta_n^\chi \to \delta$. The relative entropy typically takes a pair of probability distributions as arguments, but given that each hypothesis is concerned only with a single Bernoulli-distributed random variable uniquely specified by a a pair of real parameters (the quantities p and $p - \Delta_\epsilon$), we will use the shorthand $D(p\|q)$ for real variables p and q. In this case the relative entropy can be expanded as

$$D(a\|b) = a \ln \frac{a}{b} + (1-a) \ln \frac{1-a}{1-b}. \tag{S3}$$

Note that in the limit where $a \to 1$, using that $\lim_{a\to 1^-} (1-a)\ln(1-a) = 0$, this expression becomes

$$\lim_{a\to 1^-} D(a\|b) = \ln \frac{1}{b}. \tag{S4}$$

After rearranging the expression for the optimal asymptotic Type II error given by the Chernoff-Stein lemma, we can achieve a test with statistical power $1-\delta$ by taking a number of measurements

$$n > \frac{1}{D\left(p\|p-\Delta_\epsilon\right)} \ln \frac{1}{\delta}. \tag{S5}$$

Moreover, this bound is tight in that it gives the correct asymptotic relationship between n, D and δ; generically δ can be lower bounded ([S25], p666) such that

$$\frac{e^{-Dn}}{n+1} \le \delta \le e^{-Dn}. \tag{S6}$$

Two important limiting cases of this expression have relevance here. Firstly, if $p \gg \Delta_\epsilon$, then Taylor expanding n for small Δ_ϵ gives that it is sufficient to take

$$n \ge \frac{2p(1-p)}{\Delta_\epsilon^2} \ln \frac{1}{\delta}. \tag{S7}$$

Secondly, if $p = 1$, then it is sufficient to take

$$n \ge \frac{-1}{\ln\left(1-\Delta_\epsilon\right)} \ln \frac{1}{\delta} \approx \frac{1}{\Delta_\epsilon} \ln \frac{1}{\delta}, \tag{S8}$$

which is in agreement with the scaling previously derived in Eq. S1. These are the limiting cases of the scaling of n with Δ_ϵ. In the worst case, n scales quadratically in Δ_ϵ^{-1}; however, for any strategy where the state $|\psi\rangle$ to be tested is accepted with certainty, only a total number of measurements linear in Δ_ϵ^{-1} are required. Thus asymptotically, a strategy where $p = 1$ is always favourable (i.e. gives a quadratic improvement in scaling with Δ_ϵ) for any $\Delta_\epsilon > 0$.

[S1] 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 **438**, 643 (2005).

[S2] 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, Nature Photonics **8**, 621 (2014).

[S3] A. Laing and J. L. O'Brien, arXiv:1208.2868 (2012).

[S4] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, New Journal of Physics **14**, 095022 (2012).

[S5] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Physical Review Letters **105**, 150401 (2010).

[S6] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nature Communications **1**, 149 (2010).

[S7] G. Tóth and O. Gühne, Physical Review Letters **94**, 060501 (2005).

[S8] G. Tóth and O. Gühne, Physical Review A **72**, 022340 (2005).

[S9] T. Sugiyama, P. S. Turner, and M. Murao, Physical Review Letters **111**, 160406 (2013).

[S10] S. T. Flammia and Y.-K. Liu, Physical Review Letters **106**, 230501 (2011).

[S11] L. Vaidman and N. Yoran, Physical Review A **59**, 116 (1999).

[S12] J. Calsamiglia and N. Lütkenhaus, Applied Physics B **72**, 67 (2001).

[S13] F. Ewert and P. van Loock, Physical Review Letters **113**, 140403 (2014).

[S14] D. Mayers and A. Yao, Quantum Information & Computation **4**, 273 (2004).

[S15] M. McKague, T. H. Yang, and V. Scarani, Journal of Physics A: Mathematical and Theoretical **45**, 455304 (2012).

[S16] T. H. Yang and M. Navascués, Physical Review A **87**, 050102 (2013).

[S17] T. Sugiyama, *Finite Sample Analysis in Quantum Estimation* (Springer, 2014).

[S18] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Physical Review Letters **107**, 210404 (2011).

[S19] C. Ferrie and R. Blume-Kohout, Physical Review Letters **116**, 090407 (2016).

[S20] G. I. Struchalin, I. A. Pogorelov, S. S. Straupe, K. S. Kravtsov, I. V. Radchenko, and S. P. Kulik, Physical Review A **93**, 012103 (2016).

[S21] D. H. Mahler, L. A. Rozema, A. Darabi, C. Ferrie, R. Blume-Kohout, and A. M. Steinberg, Physical Review Letters **111**, 183601 (2013).

[S22] 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, New York, USA, 2016) pp. 913–925.

[S23] C. Bădescu, R. O'Donnell, and J. Wright, arXiv:1708.06002 (2017).

[S24] M. Hein, *Entanglement in graph states*, Ph.D. thesis, University of Innsbruck (2005).

[S25] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, 2006).