

Quantum Verification and Estimation with Few Copies

Joshua Morris, Valeria Saggio,* Aleksandra Gočanin,* and Borivoje Dakić **

As quantum technologies advance, the ability to generate increasingly large quantum states has experienced rapid development. In this context, the verification and estimation of large entangled systems represent one of the main challenges in the employment of such systems for reliable quantum information processing. Though the most complete technique is undoubtedly full tomography, the inherent exponential increase of experimental and post-processing resources with system size makes this approach infeasible even at moderate scales. For this reason, there is currently an urgent need to develop novel methods that surpass these limitations. This review article presents novel techniques focusing on a fixed number of resources (sampling complexity), and thus prove suitable for systems of arbitrary dimension. Specifically, a probabilistic framework requiring at best only a single copy for entanglement detection is reviewed, together with the concept of selective quantum state tomography, which enables the estimation of arbitrary elements of an unknown state with a number of copies that is low and independent of the system's size. These hyper-efficient techniques define a dimensional demarcation for partial tomography and open a path for novel applications.

molecules, solid-state and optomechanical devices, even with the absence of perfect control and manipulation, are already promising candidates for building new applications aside from universal quantum computing. As difficult as it is to predict how emerging technologies will be most effectively applied, one can expect to see quantum technologies with a high degree of variability in architecture and capacity (as when classical computers emerged in the 1950s), the so-called noisy, intermediate-scale quantum (NISQ).^[1] Here intermediate-scale refers to the size of the quantum processors, in the regime of tens of qubits up to a few hundred in the next decade or so. Remarkable achievements in creating larger quantum states have already been reported^[2–8] using different quantum platforms, from superconducting architectures to trapped ion systems and photonic setups. Moreover, impressive demonstrations (such as those of a computational quantum advantage) have

recently been reported by several groups that used 53^[9] and 56^[10] superconducting qubits and up to 113 photons.^[11,4]

Such rapid development and demonstration of a quantum supremacy indicate that quantum information processing is sufficiently mature that another problem, quite aside from noisy quantum systems, has begun to make its presence known with increasing frequency. While it is all very well to coherently process quantum states that reside in an exponentially large space, it means little if one cannot retrieve and validate the results of such manipulations. So begins consideration for the metrology of quantum systems. The gold standard of quantum measurement is full state tomography,^[12] wherein complete knowledge about the state is gained via measurement. Though certainly sufficient, the complexity in both measurements and computational processing power grows exponentially fast with the dimension of the quantum system.

Given that our interest in quantum information processing is this rapid growth, inserting a step that requires exponential resources seems rather counterproductive. Until very recently, however, this exponential cost was largely irrelevant as our ability to rapidly measure or classically compute vastly outstripped our ability to perform meaningful operations with more than a few qubits. Thus, simply performing full state tomography and retrieving a complete quantum state was a viable strategy. This approach was only ever practical at the very small scale of NISQ and pre-NISQ however. In the long term, fault-tolerant and noise-resistant quantum computers ought to make a complete validation of the system less important but we are far away from such feats of quantum engineering, while still being capable of

1. Introduction

In the coming decades, thanks to rapid technological advances, the probability of a new information revolution appears quite high. Quantum systems involving photons, atoms, spins,

J. Morris, V. Saggio, B. Dakić
University of Vienna
Faculty of Physics
Vienna Center for Quantum Science and Technology (VCQ)
Vienna A-1090, Austria
E-mail: joshua.morris@univie.ac.at; valeria.saggio@univie.ac.at;
borivoje.dakic@univie.ac.at

A. Gočanin
Faculty of Physics
University of Belgrade
Studentski Trg 12-16, Belgrade 11000, Serbia
E-mail: dimic.aleksandra@gmail.com
B. Dakić
Institute for Quantum Optics and Quantum Information (IQOQI)
Austrian Academy of Sciences
Boltzmanngasse 3, Vienna A-1090, Austria

 The ORCID identification number(s) for the author(s) of this article can be found under <https://doi.org/10.1002/qute.202100118>

© 2022 The Authors. Advanced Quantum Technologies published by Wiley-VCH GmbH. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

DOI: 10.1002/qute.202100118

constructing large quantum systems. Thus a gap has appeared - systems are too large for anything nearing complete tomography but not advanced enough to assume low errors.

The advantages of a complete tomography are obvious. One need make no assumptions on any properties of the target system except that it can be repeatedly produced (reinitialized) and measured. The price of such ignorance is an exponential cost in measuring, reconstructing and storing the state of the target and is naturally unsustainable as we move into the intermediate regime. But such a problem has hardly taken the quantum estimation community by surprise and many strategies exist to mitigate such a heinous complexity cost. Often, complete information is not required in many cases and when married with random sampling techniques can result in powerful verification methods^[13–29] (see also ref. [30] for general review on the topic) that probe only some specific quantities one might wish to know about a given state. To name but a few, one might wish to investigate only the presence of entanglement in a certain quantum state^[23,24] or directly estimate the state fidelity,^[31] i.e., the quantification of the overlap between prepared and ideal states. It follows naturally that reducing the amount of obtainable information comes with a lower demand in terms of experimental resources, thus making these methods more viable alternatives when the full density matrix is not needed. For clarity, we will explicitly define here that any interrogation of a quantum system which reveals information about that system is termed a partial tomography.

It appears then that a trade-off of some kind must occur. Complexity costs can be reduced in one regard but increased in another,^[30] essentially shifting the difficulty to another stage of an experiment, or we can reduce the information extracted. Ultimately, an explicit dimension dependence remains in most tasks and this serves as a problematic complication for large-scale systems. With this in mind, we concern ourselves with strategies that appear to saturate some notion of maximal information extraction, paired with a resource cost (at every stage of the protocol) that has moderate growth in the dimension. This suggests a different mode of thinking may be in order. Rather than asking how large a quantum system we can effectively probe with a given strategy, consider instead the central question of this review:

Given a limited number of interactions with a large system, how much classical information can we learn with a high degree of certainty?

This extracted classical information can take many forms and one must be careful of the kinds of questions one asks. Consider the task of entanglement detection, which may be performed indirectly by estimating the mean value $\langle W \rangle$ of an appropriate witness W and comparing it to some threshold value W_c , which requires repeated measurements on large ensembles of identically prepared quantum states. An alternative to this is a direct approach by an oracular question “Is $\langle W \rangle < W_c$?,” which potentially can be queried with a single copy. For detecting entanglement they of course produce the same answer, but estimating the expectation value is far more resource-intensive than bounding it from above in the first place. The benefit of doing so is clear, however, the question then is how to operationally reformulate the former into the latter. This process of reformulation is one of the central topics that shall form this review.

Such thinking engenders a curious divergence from the norm of quantum metrology wherein both the dimension of a system and the number of copies are seen as a given and large. On the other hand, this decision-theory centric approach that has estimation as comparable to traversing a finite tree of outcomes to arrive at a conclusion has been shown^[22–29] to yield vastly improved complexity bounds for previously challenging measurement tasks.

By rephrasing the problem of verification in this decision-theoretic way we define our starting condition as the resources of an efficient strategy, such as a limited number of state copies, and then list measurement protocols that operate within these constraints. As an illustration of the method, consider testing some properties with N copies available, where N is potentially low (e.g., few copies). Each copy may then be considered as a precious resource for measurements we are permitted to ask a quantum system in order to ascertain its properties. For example, we wish to test if the state $\rho \in A$ or $\rho \in \bar{A}$ (with $A \cup \bar{A}$ being the complete set of states) where A denotes the property being tested (as in **Figure 1**). An efficient strategy is one where the queried system is overwhelmingly unlikely to pass a test condition if it does not contain the queried property A .

The strategy is as follows. A set of carefully designed and easy-to-perform measurements $\mathbf{Q} = \{Q_1, Q_2, Q_3, \dots, Q_L\}$ that serve as queries to the system are constructed. For the k th instance of the N copies of a state, a query $q_k \in \mathbf{Q}$ is randomly chosen and applied to that instance, producing a sequence of query outcomes $\mathbf{i} = (i_1, \dots, i_N)$ for $i_k \in \{0, 1\}$. This sequence together with the sequence of chosen queries $\mathbf{q} = (q_1, \dots, q_N)$ is then passed to a decision (cost) function $S(\mathbf{q}, \mathbf{i})$ which produces a pass/fail result. We define a strategy to be efficient if it satisfies the following probabilistic expression

$$\Pr[S(\mathbf{q}, \mathbf{i}) = \text{"pass"} | \rho \in \bar{A}] \leq \exp[-\alpha(d, N)], \quad \alpha(d, N) \geq 0 \quad (1)$$

holds for a dimension d state ρ with N repetitions (queries). This deceptively simple equation is at the heart of every strategy considered in this review. Conceptually it states that any estimator is only as good as its worst-case performance which is dictated by its probability of failure, defined as a system passing a test protocol that it should fail. If this false positive probability has a functional dependence $\alpha(d, N)$ that grows in N and does not vanish asymptotically in d , for example, typically $\alpha(N, d) = O(1)N$ is dimension free, then failure is exponentially unlikely for all targets of the protocol and it is deemed efficient. This concept is schematically depicted in **Figure 1**, where the probability that the target state ρ contains the property A builds exponentially fast with the number of questions Q_k that are asked to repeated copies of ρ .

Conventionally, verification problems are distinguished from estimation problems. However, in past years there has been an opposing trend attempting to integrate both into a unified, information-theoretic framework.^[30,32] In this respect, every partial tomography task (on finite-dimensional systems) may be posed in the decision theory point of view introduced here. To clarify this point, consider verification of certain properties (e.g., presence of entanglement), the sampling complexity depends only on the required confidence $1 - \delta$, typically $O(\log \delta^{-1})$ samples are required. On the other hand, we shall consider shadow-tomography like tasks where typically one is interested in

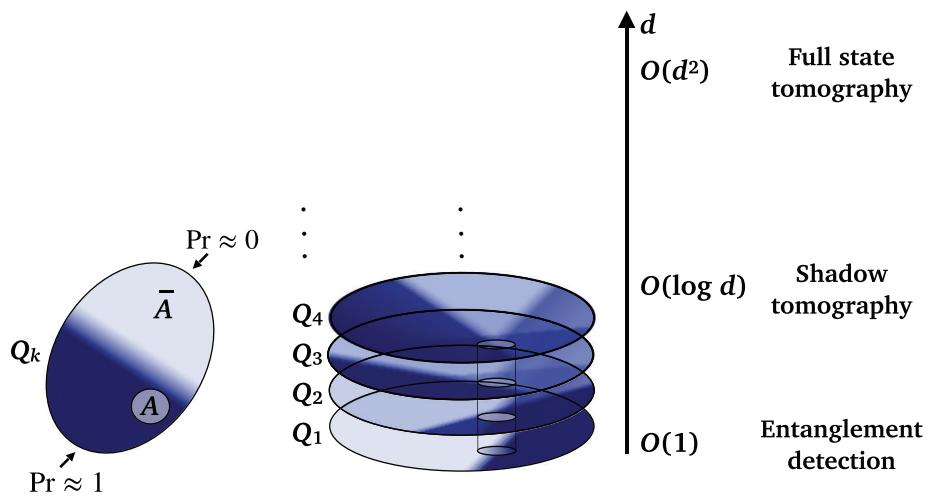


Figure 1. Schematic of the probabilistic procedure. The probability Pr that the quantum system contains the property A is found by asking relevant questions Q_k to the system. A probability close to 1 is indicated by a dark region, in contrast to a probability close to 0, associated with a lighter color. Asking more and more questions builds up the probability that the system contains A .

estimation of mean values of certain set A_1, \dots, A_M observables.^[28] To embed this problem into the decision procedure one fixes the confidence $1 - \delta$ and error ϵ and poses the estimation as a yes or no procedure: given a set of observables A_1, \dots, A_M , do their mean values lie within an ϵ interval from some (estimated) value? The set of queries Q_k is adapted to encompass the set of inequalities $|\langle A_n \rangle - \langle A_{n,\epsilon} \rangle| < \epsilon$, with $\langle A_n \rangle$ being the ground truth and $\langle A_{n,\epsilon} \rangle$ the estimated value. Assuming a good estimator, if we have preset the error value ϵ and confidence $1 - \delta$, then the procedure returns a binary outcome together with the set of estimates $\{\dots, \langle A_{n,\epsilon} \rangle, \dots\}$. The sampling complexity ranges from $O(\log M\epsilon^{-2} \log \delta^{-1})$ for protocols such as those engendered by shadow tomography to $O(d^2\epsilon^{-2} \log \delta^{-1})$ samples required for full state tomography (see Figure 1 to the right). Thus verification and estimation in this framework can be put on equal footing with the main difference being the inputs to the protocol (confidence $1 - \delta$ for verification VS confidence $1 - \delta$ and error ϵ for estimation) and their respective outputs (estimation procedure returns the set of estimates in addition to the binary yes/no output).

In a similar spirit, we require this demarcation not just in time but space as well, insisting on simple-to-implement queries on each quantum state. This will almost always mean local queries on the target system alone, rather than, for example, global (entangled) measurements on multiple instances. Finally, the computation of the decision function $S(\mathbf{q}, \mathbf{i})$ itself must also be efficient, in that it cannot have a computational complexity that depends on the system dimension in any significant way. To summarize our requirements:

- 1) Dimension demarcation: $\alpha(d, N)$ is not asymptotically small for large d , for example, $\alpha(d, N) = O(1)N$.
- 2) Fast convergence in the number of queries: $\alpha(d, N)$ grows with N for example, typically linearly.
- 3) Low computational complexity where the measurement queries Q_k are implemented by local measurement or low-depth quantum circuits.

- 4) Simple post-processing, e.g., simple evaluation of the decision function $S(\mathbf{q}, \mathbf{i})$.

This review will progress through query/answer strategies that satisfy these demanding properties in the following way. Section 2.1 constructs an explicit probabilistic detection scheme in keeping with the above framework. Section 2.2 considers what tasks may be performed using this protocol with the minimum access to a quantum state, converging on an entanglement verification protocol that uses only a single copy of a quantum state. Section 2.3 relaxes the single copy regime to that of dozens, observing the increase in information extraction possible in an experimental setting. Section 2.4 gives a brief summation of related works, accentuating the extension of our method to quantum state verification and certification. Section 3.1 considers the limit of the few-copy regime, considering the maximal amount of information one can extract from any quantum state, of any size, given a fixed number of samples. Finally, Section 4 contains a recapitulation of all important points, addressing works that go beyond techniques mentioned in the review, and discusses open questions.

2. Entanglement Verification

In searching for worthwhile tasks, it is not a contentious statement that entanglement represents a crucial resource in many quantum-information protocols.^[33] For this reason, the task of entanglement verification has by necessity spurred the development of a variety of different approaches over the past years.^[34] Traditionally, the methods of detection (see refs. [34,35] for a focused review) rely on the estimation of expectation values of observables linked to certain fundamental inequalities, such as is the case of entanglement witnesses,^[35–37] Bell inequalities^[38–40] or the use of quantum Fisher information,^[41–43] local uncertainty relations^[44] and nonlinear witnesses.^[45]

Typically, strategies will involve testing if (some function of) the expectation value(s) of some observable(s) exceeds a

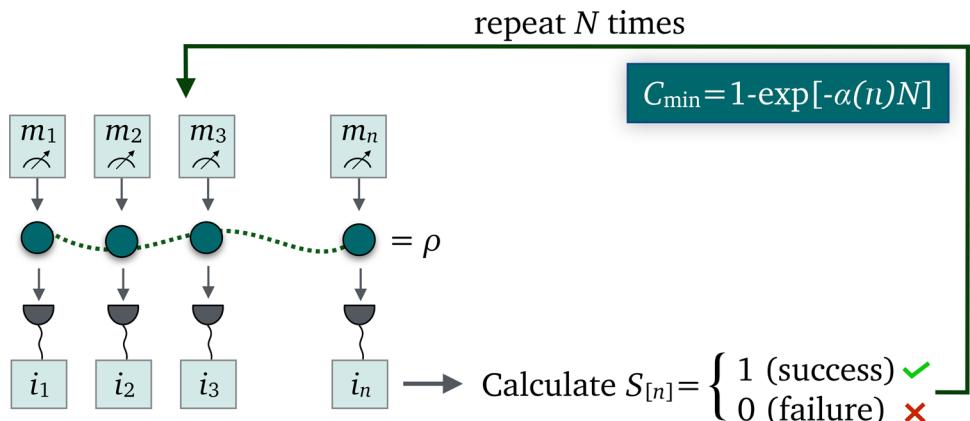


Figure 2. Probabilistic entanglement detection. A single copy of an n -partite quantum system ρ is repeatedly interrogated via random (local) measurements m_1, m_2, \dots, m_n . The performance of the system is measured via the evaluation of a cost function $S_{[n]}$. Repeating this procedure N times, the probability of detecting entanglement goes to unity exponentially fast in N for target state preparations, i.e., the (lower bound on) detection confidence grows as $C_{\min} = 1 - \exp[-\alpha(n)N]$.

certain threshold, such as testing if $\langle W \rangle < W_c$ and demanding, in practice, repeated measurements on large ensembles of identically prepared copies. This can be costly in terms of experimental requirements, scaling to impossibility with just a few steps as in photonic systems where coincidence rates fall exponentially fast in the system size.^[46] An impressive yet example of this may be found in a recent 12-photon entanglement witness experiment,^[47] where the detection rate was approximately one copy per hour. The extraction of a mean value of a single local observable, which typically requires one hundred to one thousand copies of a given quantum state, in this case, translated to an experiment duration measured in weeks. Such non-viability is a consequence of the indirect approach for testing entanglement. If instead we employ the direct method in which we pose the detection question differently, i.e., to ask: “What is the chance for the system to achieve a value $W < W_c$ in a single-shot experiment?”, we can gain a vast reduction in the detection complexity. In this respect, we will review several highly efficient methods^[23,24,26] based on the information-theoretic framework introduced in the previous section.

2.1. Probabilistic Detection Scheme

Consider a quantum system consisting of n subsystems, each residing in a finite-dimensional Hilbert space of dimension d . The first step in any partial tomography is to define the relevant set of queries Q_n that will be used to interrogate the system—as no information may be gleaned without them. Commonly these correspond to certain binary local measurements associated to yes/no questions. For the sake of generality, we include here the quantum measurements that go beyond binary logic, that is, the positive-operator valued measures (POVMs) $E_{i|m}^{(k)}$, where $\sum_i E_{i|m}^{(k)} = \mathbb{1}^{(k)}$. Here k labels the subsystem, $m \in \{1, \dots, L\}$ the local measurement setting, and i is the measurement outcome. For every subsystem, we can generate one random query associated to the setting m_k which when applied to the k th party results in some outcome i_k .

The probabilistic entanglement detection procedure, schematically shown in **Figure 2**, goes as follows:

1. A sequence of random local measurements (m_1, \dots, m_n) drawn from a prior distribution $\Pi(m_1, \dots, m_n)$ is applied to a copy of quantum state ρ to generate the sequence of outcomes (i_1, \dots, i_n) .
2. A certain binary cost function of settings and outcomes $S_{[n]} = S_{m_1 \dots m_n}^{i_1 \dots i_n} \in \{0, 1\}$ is calculated.
3. If $S_{[n]} = 0/1$ we associate “success/failure” to the experimental run.
4. Repeat N times steps 1 – 3.

The figure of merit for entanglement detection is the probability of success $P[S_{[n]} = 1]$. In essence, the cost functions are created such that this probability vanishes exponentially fast in the size of the system n and/or in the number of repetitions N for all separable states ρ_{sep} :

$$P_{\rho_{\text{sep}}}[S_{[n]} = 1] \leq \exp[-\alpha(n)N] \quad (2)$$

where $\alpha(n)$ is a function depending on the particular strategy and system’s size. On the other hand, the procedure is tailored to detect entanglement in the vicinity of some target state ρ_T , i.e., $P_{\rho_T}[S_{[n]} = 1] \approx 1$, thus, given the target-state preparations and desired detection confidence $1 - \delta$, we can estimate the average number of copies required to verify entanglement:

$$N = \frac{\log \delta^{-1}}{\alpha(n)} \quad (3)$$

It is abundantly clear that as long as $\alpha(n)$ is not vanishingly small with the size n , for example, $\alpha(n) = O(1)$, we will have a logarithmic growth of the number of copies in δ . Considering it in the opposite direction: the confidence for entanglement detection grows exponentially fast in the number of repetitions N which constitutes what we dub the few-copy detection regime^[24] where we achieve the high confidence detection by measuring only (thus the name) a few copies of the system (see Section 2.3).

The reduction of resources can be further traced down in the case where $\alpha(n)$ grows in n . In this case, for a sufficiently large system (large n) this number is reduced to the logical minimum leading to the single-copy detection.^[23,48] This possibility is presented in detail in the next section.

An important aspect of these methods is that they bypass the so-called i.i.d. (independent and identically distributed) assumption taken for granted in standard approaches. This assumption means that a source produces identical copies of a quantum state in every experimental run. This is very questionable from a practical point of view, especially given the lack of perfect control and manipulation as is the case for NISQ systems. In contrast, the shown methods surpass i.i.d. through use of random sampling a set of measurement queries. In this case, the entanglement is seen as the ability of a system to compute a certain cost function (as quantified by the probability of success) in a single-shot experiment. In such a construction of the problem, the i.i.d. requirement may be relaxed without compromising the protocol.

2.2. Single-Copy Scenario

We review the construction of the single-copy detection procedure for k -producible states^[49] which naturally extends to cluster states.^[50] Further examples include ground states for local Hamiltonians with the entanglement gap,^[51] among which we find many important classes of quantum states, such as the matrix product states^[52] and projected-entangled pair states.^[53] In all examples provided we explicitly constrain to a single experimental repetition ($N = 1$) and attempt to optimize the chance of entanglement detection. We put the main emphasis on the construction of protocol, i.e., appropriate choice of the settings and cost function.

2.2.1. Example of k -Producible Quantum State

We start with the example of the k -producible entangled state,^[49] i.e., $|\phi_1\rangle|\phi_2\rangle\dots|\phi_m\rangle$, where the products $|\phi_i\rangle$ involve at most k parties.^[54] Our aim is to show that entanglement can be detected with one copy of an n -folded state as long as n is large. To clarify the probabilistic procedure even better, we take the target state to be the product of quantum singlets $|\psi_0\rangle = |\psi^-\rangle^{\otimes n}$, where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$. The quantum singlet has the property of being the only state that returns perfect anti-correlations (the outcome -1) when measured with one of the operators $X \otimes X$, $Y \otimes Y$, or $Z \otimes Z$. Therefore, the suitable measurements to identify singlet uniquely are the following projectors:

$$Q_X = \frac{1 - X \otimes X}{2}, \quad Q_Y = \frac{1 - Y \otimes Y}{2}, \quad Q_Z = \frac{1 - Z \otimes Z}{2} \quad (4)$$

The pertinent fact is that no separable state may reveal $Q_X = Q_Y = Q_Z = 1$ simultaneously; as already emphasized, this is the unique property of the target singlet state. Thus, the maximum probability to obtain the outcome 1 for all separable inputs if measurement settings are uniformly sampled from the set $\{XX, YY, ZZ\}$ is 2/3:

$$P_{\rho_{sep}} = \langle \frac{1}{3}(Q_X + Q_Y + Q_Z) \rangle \leq \frac{2}{3} \quad (5)$$

for all separable two-qubit states ρ_{sep} . With this we can construct detection procedure for n pairs as follows: the set of $2n$ qubits is divided into consecutive pairs and for each pair, a random measurement from the set $\{XX, YY, ZZ\}$ is applied to get a sequence of results $\dots, (i_k, j_k), \dots$. From these measurement outcomes we construct the following local cost function for every pair $S_k = \frac{1}{2}(1 - (-1)^{i_k+j_k})$, where $k = 1 \dots n$ labels the qubit pair. Now, given bound (5), the relative frequency of outcome 1 shall not exceed 2/3 significantly for all separable states. Therefore, we define the overall test to be

$$S_{[n]} = \begin{cases} 1, & \sum_{k=1}^n S_k \geq (\frac{2}{3} + \epsilon)n; \\ 0, & \sum_{k=1}^n S_k < (\frac{2}{3} + \epsilon)n, \end{cases} \quad (6)$$

where $\epsilon > 0$ is a free parameter. The overall probability of success reads

$$P[S_{[n]} = 1] = P\left[S_1 + \dots + S_n \geq \left(\frac{2}{3} + \epsilon\right)n\right] \quad (7)$$

Using the standard Chernoff bound,^[55] we obtain:

$$P_{\rho_{prod}}[S_{[n]} = 1] \leq e^{-D(\frac{2}{3} + \epsilon || \frac{2}{3})n} \quad (8)$$

where $D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y} \geq 0$ is the Kullback-Leibler divergence. The probability of success vanishes exponentially fast in n for all $\epsilon > 0$. The procedure is convenient as we do not have to set ϵ in advance, i.e., we calculate ϵ as the experimental deviation of the measured sum $\frac{1}{n} \sum_{k=1}^n S_k$ from the separable bound 2/3.

In the perfect case of n singlets $|\psi_0\rangle = |\psi^-\rangle^{\otimes n}$, we shall measure $S_k = 1$ deterministically, thus we find that $\epsilon = 1/3$. The bound (8) becomes

$$P_{\rho_{sep}}[S_{[n]} = 1] \leq \left(\frac{2}{3}\right)^n \quad (9)$$

Therefore, if n is large enough, a single copy of $|\psi_0\rangle$ is sufficient to certify entanglement with high probability. For example, already for $n = 8$, the confidence level for entanglement detection is at least 96%.

Before we proceed further, let us illustrate the i.i.d. issue in the following situation. Suppose that we have only $n = 8$ qubit pairs at our disposal and we want to inspect the presence of entanglement. Given the prescription above, we may try to measure the witness operator $W = \frac{1}{3}(Q_X + Q_Y + Q_Z)$. However, it is not clear how to divide 8 pairs into three groups to measure three local observables Q_X , Q_Y and Q_Z . Also, there is no guarantee for these pairs to be in an i.i.d. state $\rho_{12}^{\otimes 8}$ which seems to be needed for separate estimation of $\langle Q_X \rangle$, $\langle Q_Y \rangle$ and $\langle Q_Z \rangle$. In this case, it is not clear how to proceed. For example, we may use the first three copies to measure Q_X , the second three to measure Q_Y , and the last two for the measurement of Q_Z . However, if the order of measurements is known in advance we may arrive at false entanglement verification: the following product state $|\phi_p\rangle = (|x+\rangle|x-\rangle)^{\otimes 3}(|y+\rangle|y-\rangle)^{\otimes 3}(|z+\rangle|z-\rangle)^{\otimes 2}$ gives exactly the same result as the i.i.d. singlet state $|\psi^-\rangle^{\otimes 8}$ for these fixed measurements. The key procedure to surpass i.i.d. assumption is random sampling and the probabilistic detection described above. It

provides a clear separation between the state $|\psi^-\rangle^{\otimes 8}$ and the product state $|\phi_p\rangle$, as the latter has only the chance of $(2/3)^8 \approx 0.039$ in the best case to reveal the result $S_1 + \dots + S_8 = 8$. In contrast, the experiment with the single-state preparation $|\psi_0\rangle$ reveals “success” always thus we verify entanglement with at least $C_{\min} = 1 - 0.039 \approx 0.96$ confidence.

2.2.2. Single-Copy Detection of Cluster States

Another example we present here is that of cluster states^[50] as a natural generalization of the previous example of k -producible state. In contrast, however, cluster states contain genuine multiparty entanglement^[56] and represent a universal resource for measurement-based quantum computation.^[57] For simplicity, we work out in detail an example of a linear cluster state (LCS); generalizations of the scheme to higher dimensions are straightforward and briefly discussed at the end of the section.

The n -qubit LCS is uniquely defined by the set of 2^n stabilizers

$$G_{q_1 \dots q_n} |LCS\rangle = G_1^{q_1} \dots G_n^{q_n} |LCS\rangle = +1 |LCS\rangle \quad (10)$$

where $G_k = Z_{k-1}X_kZ_{k+1}$ and $q_k = 0, 1$. Here $\{X_k, Y_k, Z_k\}$ is the set of standard Pauli matrices acting on k^{th} qubit and without loss of generality we have chosen the cluster state with periodic boundaries, i.e., $Z_{n+1} \stackrel{\text{def}}{=} Z_1$ and $X_{n+1} \stackrel{\text{def}}{=} X_1$.

Let us analyze a small sub-cluster of four qubits (e.g., qubits {1, 2, 3, 4}) with the corresponding stabilizers

$$G_2 = Z_1X_2Z_3, \quad G_3 = Z_2X_3Z_4 \quad \text{and} \quad G_2G_3 = Z_1Y_2Y_3Z_4 \quad (11)$$

acting exclusively on it. Even though these three stabilizers are commutative, they are not locally compatible, which means one can not measure all three simultaneously with local measurement. Therefore, there is no separable state for which $G_2 = G_3 = G_2G_3 = +1$ simultaneously. Consequently, if we randomly chose to measure one of the stabilizers (with a probability of 1/3), there is only a chance of 2/3 to get the result +1, for all separable inputs. This observation empowers our detection method to work. The strategy is to pick a random partition of the set of n qubits into 4-qubit clusters and then measure one of the corresponding stabilizers randomly on each of them. Given our previous analysis, the relative frequency of the outcome +1 cannot substantially surpass the value of 2/3. It is convenient to introduce regular partitions (i.e., neighboring clusters overlap on at most one qubit) of n -qubit cluster state into L -partition of 4-qubit clusters $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$, where c_{t_k} is the cluster consisting of the sequence of four neighboring qubits:

$$c_{t_k} = \{t_k, t_k + 1, t_k + 2, t_k + 3\} \quad (12)$$

The set of all regular partitions of size L is denoted by \mathcal{C}_L .

For every cluster c_{t_k} in the partition we associate three stabilizers:

$$\begin{aligned} G_{t_k+1} &= Z_{t_k}X_{t_k+1}Z_{t_k+2}, \quad G_{t_k+2} = Z_{t_k+1}X_{t_k+2}Z_{t_k+3} \quad \text{and} \\ G_{t_k+1,t_k+2} &= G_{t_k+1}G_{t_k+2} = Z_{t_k}Y_{t_k+1}Y_{t_k+2}Z_{t_k+3}. \end{aligned} \quad (13)$$

To each of them we associate three projectors

$$Q_{t_k} = \frac{1 + G_{t_k+1}}{2}, \quad W_{t_k} = \frac{1 + G_{t_k+2}}{2}, \quad R_{t_k} = \frac{1 + G_{t_k+1}G_{t_k+2}}{2} \quad (14)$$

projecting on the +1 outcome. To these, we associate the following measurement settings $\{ZXZZ, ZZXZ, ZYYZ\}$, and we assign “success” to the cluster measurement only if the outcome +1 (for the value of measured stabilizer) occurs. Formally speaking, for every cluster we define the following local cost function

$$S_k = S_m^{i_1 i_2 i_3 i_4} = \frac{1}{2} + \frac{1}{2} \begin{cases} (-1)^{i_1+i_2+i_3}, & m = ZXZZ; \\ (-1)^{i_2+i_3+i_4}, & m = ZZXZ; \\ (-1)^{i_1+i_2+i_3+i_4}, & m = ZYYZ, \end{cases} \quad (15)$$

where $k = 1 \dots L$. Finally, for a given partition $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ the overall cost function is represented in the following way

$$S_{[n]} = \begin{cases} 1, & S_1 + \dots + S_L \geq (\frac{2}{3} + \epsilon)L; \\ 0, & S_1 + \dots + S_L < (\frac{2}{3} + \epsilon)L, \end{cases} \quad (16)$$

where $\epsilon > 0$ is a free parameter. We associate “success” to the experimental run if the number of local successes exceeds a certain threshold of $(\frac{2}{3} + \epsilon)L$. The detection procedure goes as follows:

1. Randomly generate a partition of n -qubit cluster state $\{c_{t_1}, c_{t_2}, \dots, c_{t_L}\}$ from the set \mathcal{C}_L with a probability of $1/|\mathcal{C}_L|$.
2. Draw one measurement setting for each cluster in the partition with a probability of 1/3.
3. Perform local measurements and collect the sequence of results S_1, S_2, \dots, S_L .
4. Calculate the cost function $S_{[n]}$ by using (16).

We shall analyze the probability to pass the test for separable states. Firstly, for all product states the local cost functions S_k are independent binary random variables with $\langle S_k \rangle \leq 2/3$ for all $k = 1 \dots L$. The overall probability of success reads

$$P_{\rho_{\text{prod}}} [S_{[n]} = 1] = P_{\rho_{\text{prod}}} \left[S_1 + \dots + S_L \geq \left(\frac{2}{3} + \epsilon \right) L \right] \quad (17)$$

which is the probability that the sum of independent random variables $S_1 + \dots + S_L$ exceeds the value of $(\frac{2}{3} + \epsilon)L$. As $\langle S_k \rangle \leq 2/3$, the sum $S_1 + \dots + S_L$ cannot exceed $2/3L$ significantly. Indeed, as before, the Chernoff bound holds (for detailed proof see Supplementary Information of ref. [23]), i.e.,

$$P_{\rho_{\text{prod}}} [S_{[n]} = 1] \leq e^{-D(\frac{2}{3} + \epsilon || \frac{2}{3})L} \quad (18)$$

where $D(x||y)$ is the Kullback-Leibler divergence. As the bound holds for all product states, it also holds for their mixtures, i.e., for all separable states.

On the other hand, for the case of cluster state preparation $|LCS\rangle$, each local cost function takes the value $S_k = 1$, thus we have $\epsilon = 1/3$. The bound (18) reduces to

$$P_{\rho_{\text{sep}}} [S_{[n]} = 1] \leq \left(\frac{2}{3} \right)^L \quad (19)$$

For the sufficiently large number of qubits even a single copy of the LCS suffices to certify the presence of entanglement with high probability. For example, already for $n = 24$, we have $L = 8$ which gives a confidence level greater than 95%. Finally, let us comment briefly on the generalization to the higher dimensional case. In the case of a 2D cluster state, one can introduce partitions into 4×4 qubit clusters with the corresponding stabilizer projectors (using complete analogy to Q_{t_k} , W_{t_k} and R_{t_k} for LCS) and define the local cost functions. The 2D detection scheme also consists of drawing a random partition followed by a random measurement of local projectors on individual clusters. The separable bound similar to (18) can be derived. On the other hand, if the 2D cluster state is the input state, the probability of success is 1.

2.2.3. Single-Copy Detection of Ground-States of Local Hamiltonians

One of the strong reasons why the single-copy entanglement scheme works for the cluster states is the robustness of entanglement to local perturbations, meaning that local measurements on qubits do not destroy the entanglement between the remaining qubits completely. Thus one can expect other classes of states sharing this property to admit single-copy entanglement detection. The ground states of local Hamiltonians share this property,^[58] therefore they are good candidates. Let us consider a L -local Hamiltonian on some graph of n particles $H = \sum_{k=1}^n H^{(k)}$, where $H^{(k)}$ acts on at most L subsystems (L is fixed and independent of n). Now, let $|\psi_0\rangle$ be the ground state of the Hamiltonian $H|\psi_0\rangle = n\epsilon_0|\psi_0\rangle$, where $E_0 = n\epsilon_0$ is the ground-state energy. We are working with Hamiltonians that exhibit the so-called entanglement gap $g_E = \epsilon_{sep} - \epsilon_0 > 0$, where $\epsilon_{sep} = \frac{1}{n} \min_{\rho_{sep}} \text{Tr}H\rho_{sep}$ is the minimal obtainable energy per particle by a separable state.^[51] The main idea of the procedure is to use mean energy $\langle H \rangle$ as an entanglement witness: $\langle H \rangle \geq n\epsilon_{sep}$ holds for all separable states, while at least the ground state violates this bound. This fact can be exploited to develop an efficient probabilistic procedure by employing a tomographically complete set of measurements. In this case, the operator H translates into a classical random variable $H_{[n]}$ which serves to witness entanglement in practice (the general procedure is explained in detail in Section 2.3). The central object for our detection protocol is the following overall cost function:

$$S_{[n]} = \begin{cases} 1, & H_{[n]} \leq n(\epsilon_{sep} - \delta); \\ 0, & H_{[n]} > n(\epsilon_{sep} - \delta), \end{cases} \quad (20)$$

where $0 < \delta < \epsilon_{sep} - \epsilon_0 = g_E$ is a free parameter. Since $\langle H \rangle \geq n\epsilon_{sep}$ holds for all separable states, for the case of n being large, $H_{[n]}$ is unlikely to precede the separable bound $n\epsilon_{sep}$ in a single-shot experiment. Indeed, analogously to the previous two examples, one can derive the Chernoff bound for all separable states:

$$P_{\rho_{sep}}[S_{[n]} = 1] \leq \exp[-n\kappa^2\delta^2] \quad (21)$$

where $\kappa > 0$ is constant. Thus, for all separable inputs, the probability of success vanishes exponentially fast with n . In contrast, for the ground-state preparation $|\psi_0\rangle$, the probability of success

reaches 1 in the thermodynamic limit, as it follows from the following bound:

$$P_{\psi_0}[S_{[n]} = 1] \geq 1 - \frac{\beta^2}{n(g_E - \delta)^2} \quad (22)$$

where $\beta > 0$ is constant. The first inequality (21) is the consequence of the McDiarmid's inequality, while the second (22) is derived by using the Chebyshev's inequality. Both bounds are rigorously derived in the Supplementary Information of ref. [23].

2.2.4. Tolerance to Noise

In the end, we briefly comment on the effects of noise on single-copy entanglement detection. Consider a n -partite target state ρ_0 which passes the single-copy test with probability p_0 . In practice, one needs on average $1/p_0$ copies of ρ_0 to detect entanglement. On the other hand, let the separable bound hold, meaning that the probability of success for all separable inputs is exponentially small in n . We consider a mixture $\rho = \lambda\rho_{sep} + (1 - \lambda)\rho_0$, where ρ_{sep} is an arbitrary separable state and parameter $0 < \lambda < 1$ quantifies the amount of noise. The overall probability of success is a mixture of probabilities $P_\rho = \lambda P_{\rho_{sep}} + (1 - \lambda)P_{\rho_0} \approx (1 - \lambda)p_0$, as long as $(1 - \lambda)p_0$ is significantly larger than $P_{\rho_{sep}} = O(\exp[-nc])$. This implies that noise impacts detection by suppressing the probability of success by a factor $1 - \lambda$, for any kind of noise representable by a separable state. Therefore, one requires on average $\frac{1}{(1-\lambda)p_0}$ experimental runs to confirm the presence of entanglement. This represents a strong resistance to noise as long as $(1 - \lambda)p_0$ is not exponentially small in n . For example, if we consider $(1 - \lambda)p_0 > 0$ constant and independent of n , then we verify entanglement with a fixed cost in terms of the number of samples. This described scenario is very different in comparison with conventional detection techniques. Generally, a witnessing method tolerates noise below a certain critical point, i.e., $\lambda < \lambda_c$, meaning that if noise passes the threshold, the scheme fails to detect entanglement.

2.3. Entanglement Detection with a Few Copies

In this section, we review an entanglement detection method where the required number of copies grows logarithmically slow with the confidence as shown in Equation (3). The main goal of this section is to translate one of the most common methods for entanglement detection, that is, the one based on entanglement witnesses^[36,37] (see ref. [35] for concise review), into an efficient framework that requires only a few experimental repetitions.

What makes the witness-based technique practical is the simplicity of its detection criterion, based on a simple mean value estimation of a single (witness) observable. Specifically, an observable W is designated a witness if $\langle W \rangle = \text{Tr}(W\rho_{sep}) \geq 0$ for all separable states ρ_{sep} , while $\langle W \rangle < 0$ holds for at least one entangled state. In principle, we can construct an entanglement witness for every entangled state ρ (theorem of completeness of witnesses^[59]), which is then used to detect entanglement in a target state. While straightforward, a drawback of the method is that the witness W cannot be accessed locally, instead it must be

decomposed into a sum of local observables $W = \sum_{i=1}^L W_i$ that must be individually estimated. This means that the mean value $\langle W \rangle$ is obtained from the $\langle W_i \rangle$'s, each of which is measured in an independent experiment. The sampling complexity of the procedure is therefore dependent on the number of local terms L , which become a significant factor for generic witnesses on a large system. To overcome this problem, remarkable effort has been put into constructing entanglement witnesses whose measurement requires a smaller number of measurement settings, thus reducing the experimental requirements^[60–63] (for more references, see recent review^[34]). For example, refs. [64,65] find optimal decompositions of entanglement witnesses into a few local operators, even reducing in some cases the witness decomposition to only two local operators.^[66] However, even with a minimal number of measurement settings, this method may become inconvenient or even unfeasible simply due to the lack of sufficient number of copies of the resource state needed to extract the witness expectation value. In such cases, alternative methods going beyond mean-value extraction are required. We review here the general method developed in ref. [24] that translates the witness method into a resource-efficient probabilistic framework described in Section 2. In this scenario, the typical procedure achieves very high confidence in entanglement detection with just few experimental repetitions (copies of target state). As we shall see, the number of measurement settings involved in the local decomposition is not the crucial parameter determining the sampling complexity, in contrast to the standard belief.^[66] We also review an experiment performed with a photonic system to test the practicality of the method.^[67]

2.3.1. Embedding Entanglement Witnesses in a Probabilistic Detection Framework

The aim of this section is to review the translation of any entanglement witness into the probabilistic framework.

As previously discussed, an entanglement witness W is normalized such that

$$\langle W \rangle_s = \text{Tr}(W\rho_s) \geq 0 \quad (23)$$

for all separable states ρ_s . On the other hand, there exists at least one entangled state ρ for which $\langle W \rangle = \text{Tr}(W\rho) < 0$. The witness operator is normally tailored to detect entanglement in the vicinity of some target state for which $\langle W \rangle$ reaches the lowest possible value. We shall slightly change the general form of W and introduce the witness operator O in the following way:

$$W = \gamma_s \mathbb{1} - O \quad (24)$$

thus Equation (23) translates to

$$\langle O \rangle_s = \text{Tr}(O\rho_s) \leq \gamma_s \quad (25)$$

for all separable states ρ_s . Now O can be decomposed in terms of L local observables O_i as $O = \sum_{i=1}^L O_i$, where each O_i can be turned into a non-negative observable by adding a constant term, i.e., $O'_i = O_i + \alpha_i \mathbb{1} \geq 0$ with $\alpha_i \geq 0$. Thus we get a new witness operator $O' = \sum_{i=1}^L O'_i = \sum_{i=1}^L (O_i + \alpha_i \mathbb{1}) = O + \alpha \mathbb{1}$, with $\alpha = \sum_i \alpha_i$,

which is positive semi-definite operator. Inequality (25) translates to the new condition:

$$\langle O' \rangle_s = \langle O \rangle_s + \alpha L \leq \gamma_s + \alpha L \quad (26)$$

for all separable states ρ_s . We now write the spectral decomposition of O'_i in terms of eigenprojectors (i.e., binary observables) M_{ik} as $O'_i = \sum_{k=1}^{J_i} \lambda_{ik} M_{ik}$, where $\lambda_{ik} \geq 0$ because O'_i 's are non-negative. Here J_i counts the non-zero eigenvalues of O'_i . Since O'_i are local, M_{ik} can be as well chosen to be local operators. To simplify the notation, we define the constant $\tau = \sum_{i=1}^L \sum_{k=1}^{J_i} \lambda_{ik}$ and we set $\mu_{ik} = \lambda_{ik}/\tau \geq 0$. Finally, the witness condition (26) reads

$$\sum_{i=1}^L \sum_{k=1}^{J_i} \mu_{ik} \text{Tr}(M_{ik}\rho_s) \leq \frac{\gamma_s + \alpha L}{\tau} = p_s \quad (27)$$

for all separable states ρ_s . The last formula completely determines a probabilistic procedure for detection. Namely, since $\sum_{ik} \mu_{ik} = 1$ and $\mu_{ik} \geq 0$, these numbers are sampling probabilities for local binary observables M_{ik} . The LHS of the equation is just the probability of success to get $M_{ik} = 1$, while the RHS is the corresponding separable bound p_s . On the other hand, for target state preparations we have violation of separable bound (26) which directly translates to a different probability of success (the entanglement value) $p_e = (\gamma_e + \alpha L)\tau$, with $\gamma_e > \gamma_s$ or equivalently the deviation $p_e - p_s > 0$.

To summarize, the procedure consists of the following steps:

1. Randomly measure observables M_{ik} (with probability μ_{ik}) N times to get the sequence of results m_1, \dots, m_N ;
2. Calculate the observed success rate $S_{[N]} = \frac{1}{N}(m_1 + \dots + m_N)$.

As before, we do not expect $S_{[N]}$ to significantly exceed the separable bound p_s for all separable states, which is encapsulated into the following Chernoff bound

$$P_{\rho_{sep}}[S_{[N]} \geq p_s + \epsilon] \leq e^{-D(p_s + \epsilon || p_s)N} \quad (28)$$

On the other hand, for target state preparation we expect $S_{[N]} \approx p_e$ and thus the average number of target-state copies needed to achieve some fixed confidence $C = 1 - \delta$ is estimated as

$$N \approx \frac{\log \delta^{-1}}{D(p_e || p_s)} \quad (29)$$

This number grows in a logarithmic fashion with the required confidence and as we shall see from examples below, only a few copies are needed to detect entanglement with a very high confidence.

2.3.2. Example I: Projective Witness for Graph States

Consider the standard projective witness for a graph state $|G\rangle$:^[35]

$$W_1 = \frac{1}{2} \mathbb{1} - |G\rangle\langle G| \quad (30)$$

tailored for detection of genuine multipartite entanglement. This witness comes already in the form of (24), and it is

therefore straightforward to identify the parameter $\gamma_s = 1/2$ and the observable $O = |G\rangle\langle G|$. We also have the local decomposition $O = \sum_{i=1}^{2^n} S_i / 2^n$, where S_i are stabilizers of state $|G\rangle$ and are in general tensor products of the Pauli operators.^[68] One can therefore easily identify $L = 2^n$ and $O_i = S_i / 2^n$. The operators O_i have to be shifted for $\alpha_i = 1/2^n$ to get non-negative observables $O' = \sum_{i=1}^{2^n} (S_i / 2^n + \mathbb{1} / 2^n)$. These are already in eigenform, thus we have $J_i = 1$, $\tau = 2$, $\lambda_i = 2/2^n$ and $M_i = (S_i + \mathbb{1})/2$. The sampling probabilities are $1/2^n$ and the separable bound is calculated from

$$\sum_{i=1}^{2^n} \frac{1}{2^n} \text{Tr}(M_i \rho_s) \leq \frac{3}{4} = p_s \quad (31)$$

On the other hand, for the target state preparation $\rho_T = |G\rangle\langle G|$ we have

$$\sum_{i=1}^{2^n} \frac{1}{2^n} \text{Tr}(M_i \rho_T) = 1 \quad (32)$$

thus the entanglement value reads $p_e = 1$. To estimate the number of copies, we can choose, for example, a confidence of $1 - \delta = 0.99$. Equation (29) gives us $N \approx \log(1 - 0.99)^{-1} / D(1||3/4) \approx 16$, which is a notably small number. A naive approach of measuring all 2^n observables M_i independently will quickly become unfeasible, while with the probabilistic detection we achieve the same confidence with a constant number of copies, regardless of the system size.

2.3.3. Example II: Witness Requiring two Local Measurements

The second example we consider is the witness tailored to detect entanglement in n -qubit cluster state $|C\rangle$ presented in Ref. [66] (an equivalent example is also presented for the GHZ state which in full analogy can be adapted here). An optimal witness decomposition for detecting genuine multipartite entanglement requiring only two measurement settings is found:

$$W_2 = 3\mathbb{1} - 2 \left(\prod_{\text{even } i} \frac{\mathbb{1} + G_i}{2} + \prod_{\text{odd } i} \frac{\mathbb{1} + G_i}{2} \right) \quad (33)$$

with $i = 1, \dots, n$. The observables G_i are called generators of the state (in this case the cluster state $|C\rangle$), and constitute a subset of the stabilizing operators S_i . To translate this witness, we can apply the procedure described in Section 2.3.1. Firstly, we easily identify $\gamma_s = 3$ and $O = 2(\prod_{\text{even } i} \frac{\mathbb{1} + G_i}{2} + \prod_{\text{odd } i} \frac{\mathbb{1} + G_i}{2})$. We notice that O is already decomposed into two non-negative binary observables $M_1 = \prod_{\text{even } i} \frac{\mathbb{1} + G_i}{2}$ and $M_2 = \prod_{\text{odd } i} \frac{\mathbb{1} + G_i}{2}$ and the sampling probabilities are $1/2$. The separable bound is given by

$$\sum_{i=1}^2 \frac{1}{2} \text{Tr}(M_i \rho_{\text{sep}}) \leq \frac{3}{4} = p_s \quad (34)$$

On the other hand, the target state preparation returns $p_e = 1$ and the estimated number of copies entirely matches the analysis provided in the previous example. From here we see that although the projective witness (30) involves exponential terms in the local

decomposition, it performs equally well as the witness with two settings only.

2.3.4. Generic Witness

In the last two examples, the sampling complexity was completely independent of the system size: the average number of required copies solely depends on the required confidence for entanglement detection. However, we cannot expect such size-free behavior in the general case. The key parameter dictating the scaling behavior is the deviation between entanglement value and separable bound $p_e - p_s$, which can become asymptotically small with the size of the system. To illustrate this, we consider the example of the following witness

$$W = (N - 1)\mathbb{1} - \sum_{i=1}^n S_i \quad (35)$$

constructed to detect entanglement in the vicinity of the state stabilized by the set S_1, \dots, S_n .^[69] The translation procedure is very straightforward in this case resulting in the following separable bound

$$\sum_{i=1}^n \frac{1}{n} \text{Tr}(M_i \rho_{\text{sep}}) \leq 1 - \frac{1}{n} = p_s \quad (36)$$

where $M_i = (\mathbb{1} + S_i)/2$, while for the target state preparation we have $p_e = 1$. In this case, the estimated number of copies is $N \approx \frac{\log \delta^{-1}}{D(1||1-\frac{1}{n})}$. For large n this can be approximated with $N \approx n \log \delta^{-1}$, which defines a linear growth in the system size. In the general case, supposing that $\epsilon_0 = p_e - p_s$ is asymptotically small in n , then we have two regimes: if $p_e = 1$ formula (29) gives $N \approx \frac{\log \delta^{-1}}{\epsilon_0}$, while for $p_e < 1$ this scaling becomes quadratically worse $N \approx \frac{2p_e(1-p_e)\log \delta^{-1}}{\epsilon_0^2}$. For a generic witness, as long as $\epsilon_0^{-1} = \text{poly}[n]$, the procedure remains efficient.

2.3.5. Experimental Scenario

The theoretical framework presented above was tested in the experiment presented in ref. [24]. The setup was designed to produce the following six-photon cluster state

$$|Cl_6\rangle = \frac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle) \quad (37)$$

which is an equivalent version (up to local unitary transformations) of the six-qubit H-shaped cluster state depicted in Figure 3a. The state is produced with a photonic setup where logical qubits are encoded in the photons' polarization. The entanglement verification test was performed both for witnesses W_1 and W_2 introduced in Equations (30) and (33). The binary observables M_i defining the witness W_1 were sampled $N = 160$ times, while the M_i constituting W_2 were drawn $N = 150$ times. The observed deviation $\epsilon = S_{[6]} - 3/4$ from the separable bound was plugged into Equation (28) to put the lower bound on the confidence for entanglement detection. Figures 3b,c provide the experimental

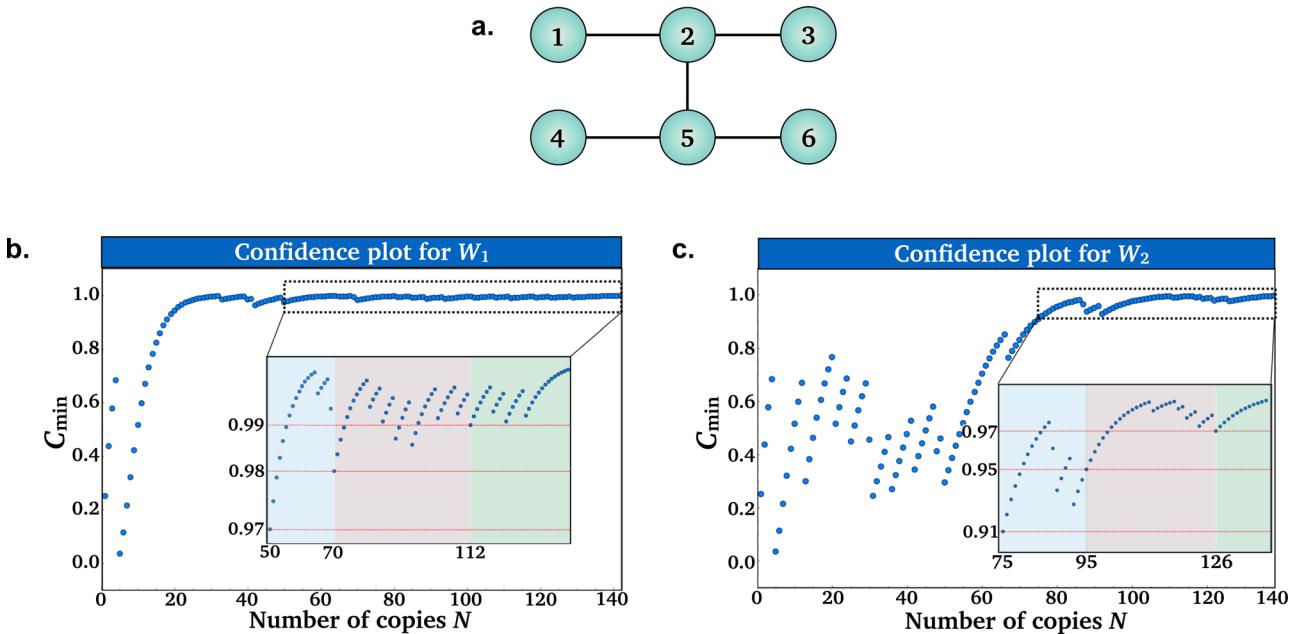


Figure 3. Experimental scenario. a) H-shaped six-qubit cluster state. Each disk represents a qubit prepared in the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and the solid lines indicate entanglement between them. b,c) Growth of the minimum confidence with the number of copies. The blue dots represent C_{\min} , calculated from equation (29) for W_1 (b) and W_2 (c). The insets show the region where the confidence stabilizes. Adapted with permission.^[24] Copyright 2019, The Author(s), under exclusive licence to Springer Nature Limited.

plots for the two witnesses. In the case of witness W_1 , the plot in Figure 3b shows that only 50 copies of the experimental state are needed to verify genuine multipartite entanglement with at least 0.97 confidence, and that 112 suffice to reach at least 0.99. In the same way, using the witness W_2 , it is visible from Figure 3c that 126 copies are enough to reach a confidence of at least 0.97. The deviation from the expected theoretical values is due to experimental imperfections that lead to a limited fidelity of $F \approx 0.75$.

2.4. Related Work

Probabilistic detection techniques similar to those presented here can be found in several other works. In the context of Bell's inequalities, similar kinds of probabilistic protocols are constructed for the single-shot non-locality detection^[70] and entanglement detection via preparation games.^[71] In the context of quantum state verification,^[18,72–74] a single-shot entanglement verification naturally arises in bipartite states as long as the dimension of marginal systems becomes sufficiently large.^[75,76] The generalization to the GHZ states can be found in ref. [77]. These results show a more intimate relation between our probabilistic detection and quantum state verification protocols. This is supported by the fact that our probability of success (to calculate the cost function) is usually maximized to 1 for the target state, thus the correct set of outputs does not witness only the presence of entanglement, it also indicates that the preparation state is close to the target state. Therefore, it seems that our protocols naturally extend from entanglement detection to more informative quantum state verification without significantly increasing the cost in terms of resources. Given this relation, we will review

in what follows the basics of quantum state verification and its recent extension to the device-independent scenario and quantum state certification.^[27]

2.4.1. Quantum State Verification and Certification

The quantum state verification (QSV) is a protocol that verifies if an unknown input state is close (in fidelity) to some target state. Due to its simplicity and low complexity, it has recently attracted a lot of attention in the community, and several verification protocols have been constructed for various classes of states^[20,26,74,78–80] together with experimental demonstrations.^[72,81,82] From the theoretical point of view, QSV plays an important role in protocols such as blind quantum computation and quantum networks.^[83–90]

In this section, we recall the framework for QSV as defined in ref. [18]. The main goal is to verify if a sequence of states $S_N = \{\sigma_1, \dots, \sigma_N\}$ is close to the target state $\sigma = |\psi\rangle\langle\psi|$ by using only local measurements. The measurement strategy labeled by Ω thus consists of L different local measurements $\{M_{i|m}\}$, where $m \in \{1, \dots, L\}$ labels the setting and $i \in \{0, 1\}$ the binary outcome. In the k th round a measurement from Ω is randomly sampled (with probability p_k) and applied to the state σ_k . We say that the state σ_k passed the round if it returned the output $i = 1$. Otherwise, we say it failed. The first time a round is failed the process is aborted. The measurements are chosen such that the strategy operator $\hat{\Omega} = \sum_m p_m M_{1|m}$ is uniquely optimized for the target state: $\hat{\Omega}|\psi\rangle = +1|\psi\rangle$, meaning that only target state passes all verification rounds with probability 1. Under the premise that all emitted states are either $\langle\psi|\sigma_k|\psi\rangle \leq 1 - \epsilon$ away from target

state or all of them are actually target states $\sigma_k = |\psi\rangle\langle\psi|$, one can derive the average number of tests $N = \frac{\log \delta^{-1}}{v(\Omega)\epsilon}$ needed to achieve the confidence of $1 - \delta$. The value $v(\Omega)$ is the so-called spectral gap which is the second largest eigenvalue of $\hat{\Omega}$.

The sampling complexity of the QSV is only up to a constant factor optimal in error ϵ , as the best strategy is achieved for the projection on target state measurement $\{|\psi\rangle\langle\psi|, 1 - |\psi\rangle\langle\psi|\}$ resulting in $\sim \frac{\log \delta^{-1}}{\epsilon}$ scaling. While this is a remarkable result, the downside of the QSV scheme as proposed by^[18] is its impracticality, i.e., the verification condition of all states either being $1 - \epsilon$ away from the target or all being target states. Such assumption is very hard to justify operationally and extremely hard to achieve in laboratory.^[81] In our recent work, we relax this assumption and we fully adapt the protocol to device-independent (DI) quantum state verification.^[27] In this case, all devices are not characterized nor trusted and all operations are treated as black-boxes.^[91–94] Remarkably, we have shown that the optimal scaling of $N = O(\frac{\log \delta^{-1}}{\epsilon})$ translates to the DI scenario. The scheme is more practical as it tolerates $O(\epsilon)$ failure events during the verification process without losing the optimal scaling.

A general drawback of QSV is that the verification process destroys the quantum resource and the conclusion is made about the resource which is fully consumed. This prevents the possibility of using it for other protocols and further processing. The solution to this problem is found in quantum state certification: a protocol in which a fragment of the resource copies is measured to authorize the rest of the copies. The pioneering quantum state certification protocols are developed in refs.[75,76]. In these works, one explores permutation symmetry and measures all but one copy, which then serves as a certificate. The protocol is very powerful as it applies to a generic adversarial scenario, but it unfortunately consumes $O(N)$ resources to certify a single copy only. Our new approach on DI QSV developed in ref. [27] fully extends to quantum state certification. There a reliable certification scheme is provided for the case of independent copies to large certificates, e.g., consisting of $O(N)$ copies. Unfortunately, the full adversarial scenario is still unresolved and remains for future investigations.

3. Universal Data Records and Partial Tomography

We have seen that in the limit of tens of copies, one can still construct powerful techniques that extract surprisingly sophisticated conclusions on unknown quantum data. We end this review by considering the limits of such extraction, that is, what is the limit of information one can know about an arbitrarily sized state given a constant number of copies of that state? Many things we might wish to know may be formulated as some kind of partial tomographic task, for example, “Is the state entangled?” or “Is the state ϵ -close to some target quantum state?”. With so many possible questions for the same target, we might ask ourselves how many of them can be determined in parallel? Can it be done efficiently or rather, can we accurately extract multiple classical features from a moderate number of data samples?

Suppose now we introduce another “resource” to manage in our pursuit of efficient query protocols; our own indecision. If we do not a priori know what classical information we wish to extract from our target quantum system, what choice of mea-

surements maximizes our knowledge at a later point? Since our choice is made a posteriori, then all possible questions we could ask a state are equally possible and so we must take some kind of universal data samples that best approximates the space of all possible future queries. This is certainly achievable via full state tomography. Tomography schemes abound that aim to attack the difficulty of this task through this tactic, however, a seemingly unavoidable fact of estimating properties of an arbitrary density operator is the required polynomial number of measurements in the dimension d . More precisely, achieving an absolute error ϵ in the estimation of an unknown density matrix requires at least $O(d^2\epsilon^{-2})$ ^[28] copies of a quantum state. This has to be combined with post-processing which requires storing and manipulation of exponentially large matrices. Such tasks are certainly beyond the scope of large quantum systems.

However, full state tomography may provide more information than actually needed. Our task may not require the computation of any feature of a quantum state but some more restricted class. Clearly, there is a resource-gain trade-off relation as further knowledge requires further resources, but one can get surprisingly far extracting interesting properties of the system while needing very little resources. The most significant development towards addressing this problem in recent times is due to Aaronsen^[28] breakthrough. Within it he describes a protocol dubbed “shadow tomography,” wherein an exponentially sized list (of mean values) of binary observables on a quantum state of dimension d (mixed or otherwise) may be estimated to high precision using a measurement sample of $O(\log d)$ size.

The name is derived from the idea that one is not especially interested in the entire quantum state but rather its projections onto a fixed set of observables—the lower dimensional “shadows” of a quantum state. With this in mind, suppose we wish to estimate a set of M linear features $\{\text{tr}[\rho E_1], \dots, \text{tr}[\rho E_M]\}$ with as few copies of ρ as possible. Rather surprisingly, shadow tomography shows that M can be exponentially large with only a polynomial resource overhead. This statement is certainly worthy of consideration given our original problem. The main result of Aaronsen paper is the following theorem:

Theorem 3.1 (Aaronsen^[28]). *Shadow tomography is solvable using only*

$$N = \tilde{O}\left(\frac{\log 1/\delta}{\epsilon^4} \cdot \log M^4 \cdot \log d\right) \quad (38)$$

copies of the target state ρ where the \tilde{O} hides a polylog factor. The procedure is fully explicit.

The consequences of this should be readily apparent given the preceding review. A set of binary observables $\{E_1, \dots, E_M\}$ on an arbitrary quantum state can be estimated to within an ϵ absolute error with probability $1 - \delta$ using a number of samples that grows logarithmically with the dimension and size of the estimated set. We direct interested readers to the original paper for proof of the above theorem and content ourselves here with answering why this does not immediately solve the problem of partial tomography. Though shadow tomography is theoretically efficient in most of the required categories, namely in terms of sample number, computational complexity and memory complexity, it unfortunately fails when considering the sophistication

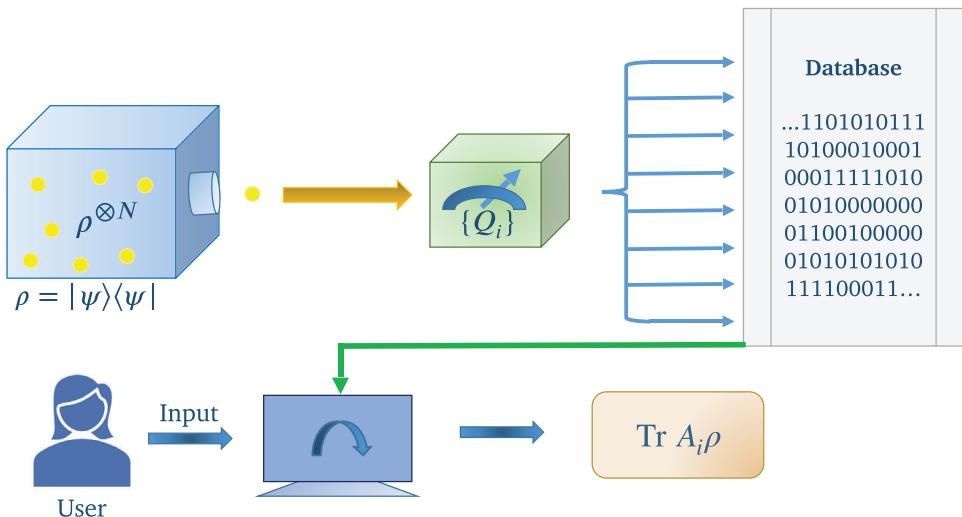


Figure 4. Protocol for estimation on demand. The central idea is based on a two-stage procedure: data acquisition and post-processing. In the first phase the universal data record of size N is collected via some kind of universal POVM (e.g., information complete measurement). In the second phase, an user chooses on demand certain features to extract (e.g., from a continuous class). A simple post-processing (low memory and computation) of the collected data furnishes the task, resulting in estimation confined to an absolute error of $O(\frac{1}{\sqrt{N}})$. Every new estimation (from the same data) comes at the logarithmic cost thus enabling extraction of M features with the $\log M$ overhead.

of the required measurements. The protocol requests joint measurements to be made on tensor products of the target state of a size $\epsilon^{-2} \log d$, which are repeatedly measured using carefully performed non-demolition measurements,^[95] themselves a difficult procedure to perform in experiments. It is worth noting that it is not shown that these resource demands are strictly required for the protocol and indeed this was not a stated goal of the work.

We review here two protocols that go beyond these limitations: selective quantum state tomography^[29] and classical shadows.^[22,25] The main emphasis here is on low-cost implementation and a universality property: we ask for the possibility of extracting on demand (a posteriori) arbitrary features (from a given class) of a quantum state from some kind of universal data record of moderate size. To illustrate this, suppose we wish for a protocol that allows for efficient estimation of a (finite) selection of observables from a continuous class—after our experiment is complete. On the surface this seems a monstrous request to make and one that can only begin to be fulfilled by a full-state tomography. Ultimately, we shall see how this is done (for a class of bounded observables) with a cost that is completely dimension independent and requires a resource complexity that is $\log M$ for M different features (a linear cost in exponentially many). The general protocol is illustrated in **Figure 4** and it reassembles the one defined in the introductory section with the difference being the possibility of re-using the same data (a universal record) to estimate on demand (a posteriori) a feature from some predefined (continuous) class of features. The protocol is described concretely in subsequent sections.

3.1. Selective Quantum State Tomography (SQST)

Our task now is to weaken the stringent requirements on the measurements required for shadow tomography while still be-

ing able to estimate many operators simultaneously. To begin, let us settle for simultaneous estimation of the unit operators $A_{ij} = |j\rangle\langle i|$, where $i = 1 \dots d$ and d is arbitrarily large. The expectation values of these operators correspond to the density operator element ρ_{ij} . A naive one-by-one measurement strategy is obviously inefficient here, as estimation of another unit operator may then require an entirely new set of measurements resulting in the general cost growing with the dimension of the system d . On the other hand, if one estimates various functions from the same data sample, wherein each individual estimation is efficient in the sense of a Chernoff-like bound (1), then we can ensure the accuracy of multiple estimations within the fixed overall error only at the logarithmic cost $\log M$ for M parallel estimations (this follows from a simple union bound^[96] for multiple random variables). This point is the crux of the protocol - once a sufficient set of measurements have been generated for a universal data record (see **Figure 4**), any density matrix element ρ_{ij} can be estimated on demand at guaranteed precision from identical data. To do this without the complexity of measurements demanded by shadow tomography requires the introduction of a special POVM based on mutually unbiased bases.^[97]

To construct the protocol, we shall first pick an adequate set of measurements. The set of all matrix units A_{ij} forms a basis in the operator (Hilbert-Schmidt) space, thus the universal data record has to be constructed from an informationally complete POVM. The simplest and most practical choice is local measurements which are sufficient for information completeness in general but they are of limited applicability in the context of partial tomography.^[22] Thus one needs entangled measurements in general, keeping in mind that these shall be of a low computation complexity (i.e., implementable via low-depth quantum circuits).

The first such basis that springs to mind is one built from mutually unbiased bases (MUBs). MUB sets are groups of orthogonal bases defined on a finite dimensional (of dimension d)

Hilbert space. They hold the special property whereby any two basis elements $|i, m\rangle$ and $|j, n\rangle$ drawn from different bases – indexed as m and n – have a constant inner product $|\langle i, m|j, n\rangle|^2 = 1/d$, $\forall m \neq n$. Here $i, j = 1 \dots d$ index the basis elements, while $n, m = 1 \dots d + 1$ label the basis. While there are infinitely many complete MUBs for a given dimension, we are always free to apply a global unitary to each element of the set, transforming them into another pure state while maintaining the inner product between elements. Due to this, we will always choose the $m = 1$ basis to be the computational basis and define the remaining bases in terms of this set

$$|k, m\rangle = \frac{1}{\sqrt{d}} \sum_{l=1}^{d-1} \alpha_l^{km} |l, 1\rangle; \quad m \neq 1 \quad (39)$$

with $|\alpha_l^{km}| = 1$. The specific form of α_l^{km} is dependent on the dimension of the underlying Hilbert space, with different expressions for prime^[98] and prime power^[99] dimensions. To proceed we use a useful fact^[99] about arbitrary operators A acting on the same space our MUB is defined upon, namely that

$$A = -\text{tr}(A) \mathbb{1} + \sum_{m=1}^{d+1} \sum_{k=1}^d O_k^{(m)} \Pi_k^{(m)} \quad (40)$$

with $O_k^{(m)} = \text{tr}[A \cdot \Pi_k^{(m)}]$. The $\Pi_k^{(m)}$ are constructed from the basis elements of the MUB such that $\Pi_k^{(m)} = |k, m\rangle\langle k, m|$. The presented decomposition proofs information completeness of MUBs and we can define the corresponding POVM as $\{R_k^{(m)} = \Pi_k^{(m)} / d\}$ with k, m indexed as before.

A particularly critical example may be found in the matrix unit operators. Let $A_{ij} = |j\rangle\langle i|$ with $|i\rangle$ defined in the computational basis and $i \neq j$. Their decomposition (40) adapted to the POVM elements reads

$$A_{ij} = \sum_{k=1}^d \sum_{m=2}^{d+1} \eta_{ij}^{km} R_{km} \quad (41)$$

Here $\eta_{ij}^{km} = \alpha_i^{km*} \alpha_j^{km}$, thus $|\eta_{ij}^{km}| = 1$ which is the crucial property. Since $\langle A_{ij} \rangle = \text{tr}[\rho A_{ij}] = \rho_{ij}$, measuring a particular operator element ρ_{ij} amounts to estimating the expectation value of A_{ij} . Given the decomposition above, the mean values $\langle A_{ij} \rangle$ are equivalent to the expectation value of the random variable $\eta_{ij}^{(s)} \in \{\eta_{ij}^{km} \mid m = 2 \dots d + 1, k = 1 \dots d\}$, associated with outcomes of the POVM $\{R_k^{(m)}\}$. Practical implementation of this POVM amounts to randomly choosing one of d orthonormal basis sets (not including $m = 1$) to measure a copy of ρ in, each with probability $1/d$ of being selected. A tomography to estimate ρ_{ij} would then proceed by the generation of N copies of ρ , each measured using this POVM. For each measurement outcome, indexed by s , we update an approximation to the above sum as the following estimator

$$\rho'_{ij} = \frac{1}{N} \sum_{s=1}^N \eta_{ij}^{(s)} \quad (42)$$

To be completely explicit, a selective quantum state tomography would proceed in the experiment as follows:

- 1) Measure a copy of the quantum state ρ using the POVM defined by $\{R_k^{(m)}\}$, to get the measurement result (k, m) .
- 2) Repeat the procedure N times to get the (universal) measurement record of outcomes $\{(k_1, m_1), \dots, (k_N, m_N)\}$. This concludes the experimental phase of the SQST.
- 3) In post-processing, choose a particular element ρ_{ij} to compute $\eta_{ij}^{(s)}$ and the sum in Equation (42).
- 4) To estimate a different element ρ_{st} , simply update the values of i, j to s, t and recompute the estimator, without further measurements.

If we calculate the number of state copies N of ρ required for the estimator ρ'_{ij} to converge to ρ_{ij} within some error ϵ and failure probability δ . Though $\eta_{ij}^{(s)}$ is complex, we may still apply the usual concentration inequalities by considering $\eta_{ij}^{(s)}$ as two bounded random variables such that $|\Re[\eta_{ij}^{(s)}] + i\Im[\eta_{ij}^{(s)}]| = 1$. Recall that $\rho'_{ij} = N^{-1} \sum_{s=1}^N \eta_{ij}^{(s)}$ and note that $\mathbb{E}[\rho'_{ij}] = \rho_{ij}$. Following a concentration inequality approach, we wish to compute the bound $\Pr(|\rho'_{ij} - \mathbb{E}[\rho'_{ij}]| \geq \epsilon)$. First, we will isolate the real and complex components of the random variable $\eta_{ij}^{(s)}$. By the triangle inequality, we have that

$$\Pr\left(\left|\rho'_{ij} - \mathbb{E}[\rho'_{ij}]\right| \geq \epsilon\right) \leq \Pr\left(|A| \geq \frac{\epsilon}{\sqrt{2}}\right) + \Pr\left(|B| \geq \frac{\epsilon}{\sqrt{2}}\right) \quad (43)$$

for $A = \text{Re}(\rho'_{ij}) - \mathbb{E}[\text{Re}(\rho'_{ij})]$ and $B = \text{Im}(\rho'_{ij}) - \mathbb{E}[\text{Im}(\rho'_{ij})]$. From here, we may apply a standard Hoeffding's inequality for bounded random variables to each term individually to get

$$\Pr\left(\left|\rho'_{ij} - \mathbb{E}[\rho'_{ij}]\right| \geq \epsilon\right) \leq 4e^{-\frac{N\epsilon^2}{2}} = \delta \quad (44)$$

We may then deduce the number of copies $N = O(\epsilon^{-2} \log \delta^{-1})$ required to estimate ρ_{ij} with an error bound $|\rho'_{ij} - \rho_{ij}| < \epsilon$ that occurs with probability greater than $1 - \delta$. This is in tandem with an $O(N)$ complexity overhead in both the required memory and computation, given we need only to store the outcomes of each measurement and the summation may be computed piece-wise. For estimation of any ρ_{ij} , we need also to account for the diagonal case $i = j$, something we neglect in the above formulation of SQST. Fortunately, the estimation of the diagonal elements of ρ_{ii} is straightforward. This stems from the fact that diagonal estimation of density operators is something of a simple case, achievable with measurement in the computational basis. For truly arbitrary estimation of the elements of a density operator we thus need to maintain two measurement records; one for the diagonal elements which gives the ρ_{ii} directly, and another for the off diagonals ρ_{ij} , both requiring $N = O(\epsilon^{-2} \log \delta^{-1})$ copies of the state. Finally, an additional factor must be included if multiple elements are ρ_{ij} to be estimated, corresponding to M repetitions of step 4 in the experiment. This amounts to $\log M$ overhead which comes from the union bound resulting in $N = O(\epsilon^{-2} \log \delta^{-1} \log M)$ repetition. Remarkably, this scaling is free of the dimension d .

3.2. Relation to Full Tomography and Arbitrary Observables

It is tempting to conclude that if one can efficiently estimate all individual elements of a density operator more efficiently than one can estimate the density operator itself efficiently. This is true but only in a technical sense—while SQST will give a bounded error on individual elements with high probability, the overall error of the estimated quantum state in the usual metrics—namely trace distance—may be exponentially large. This comes from SQST estimation error being equivalent to the max norm $\|E\|_{\max} := \max_{ij} |E_{ij}| \leq \epsilon$ which is related to the trace distance norm via

$$\frac{1}{\sqrt{d^3}} \|E\|_1 \leq \|E\|_{\max} \leq \|E\|_1 \quad (45)$$

This is rather unsurprising as anything else would imply a protocol that outperforms provably optimal full state tomography.^[28] Of course, it is still possible to perform state tomography in the supremum norm. In a similar manner to maximum likelihood estimation, a semidefinite program

$$\rho_p := \underset{\sigma \geq 0}{\operatorname{argmin}} \| \rho_L - \sigma \|_{\max} \quad (46)$$

may be constructed that yields positive semi definite solutions from the data record generated by SQST.^[29] Though running such an optimization program would not be computationally efficient, the required sample complexity for all d^2 elements remains efficient at $\log d^2 = 2 \log d$.

Another interesting point to investigate is the application of SQST to estimate mean values of observables going beyond matrix units $|j\rangle\langle i|$. Consider a general decomposition given in Equation (40) of an operator A

$$A = \sum_{k=1}^d a_{kk} \Pi_k^{(1)} + \sum_{m=2}^{d+1} \sum_{k=1}^d a_{km} \Pi_k^{(m)} = A_0 + \tilde{A} \quad (47)$$

where we intentionally separate decomposition into computational basis which gives diagonal matrix A_0 and the rest of \tilde{A} with all 0 on the main diagonal. Furthermore, we restrict our attention to operators bounded in entrywise 1-norm $\|A\|_1 = \sum_{ij} |a_{ij}|$, where a_{ij} are matrix elements of A in the computational basis. Given $\|A\|_1$ bounded we have all elements $|a_{ij}| \leq \|A\|_1$ also bounded. As before, the estimation is broken into two stages: estimation of A_0 which is efficiently done on computational basis (since a_{ii} are bounded) and estimation of \tilde{A} which is performed by random sampling of MUBs (see the previous section). The corresponding random variable a_{km} is bounded, i.e., $|a_{km}| = |\text{tr}[A' \Pi_k^{(m)}]| \leq d \sum_{ij} |a_{ij}| |\langle i, 1 | k, m \rangle \langle k, m | j, 1 \rangle| \leq \|A\|_1$, thus the efficiency of the estimation follows from the Hoeffding bound of Equation (44) with $N = O(\epsilon^{-2} \log \delta^{-1} \|A\|_1^2)$.

The previous analysis shows that operators bounded in entrywise l_1 -norm can be efficiently estimated by the SQST procedure. However, these bounds are not optimal. To see this, suppose we simultaneously estimate the mean values of $4^n - 1$ Pauli operators (excluding identity) $A = \sigma_1 \otimes \dots \otimes \sigma_n$, where σ_k is one of the standard Pauli matrices. We have $\|A\|_1 = d = 2^n$, thus our previous analysis predicts a sample cost of $N = O(4^n n)$, where the factor $n \sim \log 4^n$ comes from the union bound. However, it is

well known^[100] that the set of $4^n - 1$ Pauli operators can be factored into $2^n + 1$ groups each composed of $2^n - 1$ commuting operators with their common eigenbases being MUBs. This means that a single MUB measurement can return all 2^n mean values (of commutative Paulis) at the cost of $O(n)$ thus the estimation of all 4^n requires $O(2^n n)$ copies (to measure all in MUBs). This scaling is known to be optimal.^[101] Consequently, this is quadratically better than the estimation given by the norm $\|\cdot\|_1$ analysis meaning that the derived bounds can be further improved. One way of doing this is to employ the Bernstein's inequality^[102,103] which controls also the variance of the random variable thus leading to potentially better bounds. Another possibility to generically improve the scaling is to change the POVMs and type of estimator, e.g., instead of a simple linear estimator, one may use the median of means estimator.^[104] This coincides with the next and final scheme in terms of sample complexity and is superior in terms of measurement complexity and efficiency for estimation of a general observable bounded in Frobenius norm. Along with SQST the next scheme called classical shadows^[22,25] is an entirely new regime of partial tomography not previously possible.

3.3. Classical Shadows

With shadow tomography suggesting the possibility of a sample-efficient universal algorithm and SQST demonstrating that a degree of generality can still be achieved with vastly simpler measurements, we close this review with the current state of the art in efficient quantum tomography. Considering again the protocol above, we defined an alternative scheme using a generalized measurement basis - the mutually unbiased bases, producing a partial tomography protocol that can construct many independent linear functions on a target state while remaining resource-efficient.

One now wonders why this was the case—a choice of unbiased bases as a first target for universal measurements is intuitive given that they form an informationally complete POVM and their very nature of containing minimal measurement bias, but they work unexpectedly well for an educated guess. A possible reason for this lies in a so-far unmentioned MUB property, namely that they form a t -design of degree two.^[105] While a full description of t -designs is unnecessary here (see ref. [106] for a complete treatment in the context of quantum mechanics), it is sufficient to understand that a quantum t -design is a probability distribution that approximates polynomial functions of order t over the complete distribution for some set. A simple (classical) example is the average of some polynomial function over the real sphere.

The relevance of this here is that such designs can be used to approximate the probability distributions of a generalized measurement basis. Higher order designs better reproduce the key properties of a distribution with a two design correctly producing the same expectation value and a three design correctly showing the same sample variance. The natural and immediate question is what do higher order t -designs yield? We clearly see from the Bernstein inequality that the variance of an observable plays a heavy role in terms of the efficiency of an estimator, so one may presume that a t -design that reproduces both the correct expectation value and variance of the approximated distribution will have improved performance again.

Coupled with a statistical trick known as the median-of-means,^[104] this is the strategy of Keung et al.^[22] who show that through randomized Clifford measurements (a three-design) they are able to estimate M observables at a number of samples that grows as

$$N = O\left(\frac{\|A\|_{max}^2 \log M}{\epsilon^2} \log \delta^{-1}\right) \quad (48)$$

with $\|A\|_{max} = \max(\|A_1\|_2, \dots, \|A_L\|_2)$ being the maximum two-norm (Frobenius) of the M observables to be estimated. Included within this bound are entanglement witnesses and fidelity estimation, both of which can be performed efficiently regardless of the system size. With regards to a two design, a three design (when coupled with sufficient statistical methods) is slightly more expensive in terms of gate complexity, requiring a cubic number of Clifford gates to achieve sufficient randomness over the Haar measure as compared to the linear cost of generating MUB measurements. Both may be considered computationally efficient however and one gains a powerful advantage when the use of a three-design Clifford measurement is allowed.

4. Concluding Remarks

In this work, we have reviewed recent approaches to answering queries of quantum states of increasing size, while avoiding an unacceptable overhead in resources. By first considering efficient tomography to be a series of queries that become exponentially unlikely to pass for all states excepting those that answer positively, we showed how this leads to hyper-efficient protocols. We demonstrated this through high-performance entanglement detection using a single copy of a quantum state; a counter-intuitive result for an estimation protocol. This was then extended by showing how the same protocol can be used for cluster states, a specific class of quantum state and the ground states of local Hamiltonian.

We proceeded to the case where a limited number of state copies is available, one can work in the few-copy regime and observe the presence of entanglement in the state with a protocol to translate any entanglement witness into a probabilistic framework. We showed that this scenario is well-suited for experimental implementations by reviewing an application to a photonic six-qubit cluster state. By demonstrating that the method provides the ability to detect quantum entanglement with very high confidence with only about hundreds of state copies, the extremely low requirements in terms of time and experimental resources were confirmed.

With experimental viability in mind, we gave a description of shadow tomography which set the stage for Selective Quantum State Tomography, showing how a special choice of POVM leads to the efficient estimation of a wide class of linear quantum functionals. This in turn leads to the current state of the art for partial tomography, a t -design based protocol using the classical shadows of a quantum state which leads to efficient estimation of an exceptionally large class of observables.

This high performance is most clearly seen in the context of possible partial tomographies performed; namely fidelity estimation (where the observable is another density operator), entangle-

ment witnesses and entropies, correlation functions up to order two and the energies of many-body local Hamiltonians.

Beyond the methods presented in this review, it is fair and also worth mentioning novel techniques that instead employ machine learning to reduce the verification requirements. In fact, the use of machine learning for quantum applications is in general experiencing rapid progress and proving useful in tasks like entanglement detection using neural networks^[107,108] or unsupervised learning^[109] and quantum state tomography using neural networks.^[19] It is also relevant that a comparable method (to SQST) for estimating elements of a density matrix exists in the continuous variable (CV) regime. Here, it is known that the estimation error depends directly on the energies,^[110,111] i.e., the estimation error for a matrix element ρ_{nm} increases with n and m (n, m index the energy eigenstates). Notably, the same behavior is not observed in SQST of discrete systems, which forms a point of interest for developing tomographic strategies targeting CV systems.

Our main focus in this review was on sampling (in terms of measurement complexity) where the presented techniques exhibit a dimensional independence, a property that is crucial for real application. There are however a number of open questions that remain to be addressed in future work. In the context of entanglement detection one immediately realizes that verification models tend to be tailored to detect entanglement in the vicinity of a target state which requires some prior knowledge of the state preparation. Which witnesses and corresponding verification procedure should one use then if there is no such prior knowledge? This is an open research topic and not many results may be found in the literature, owing to the difficult nature of this restriction. In such cases, one promising direction may be to use the method of so-called random correlations,^[112–114] which was developed for entanglement detection and try to incorporate it into the decision-theoretic framework presented here.

Another pressing issue is the assumption of “IIDness” (identical and independently distributed) samples which is highly questionable in the context of near-term quantum devices given high error rates, source drifts and lack of control and manipulation. Our entanglement detection schemes surpass the IID limitation by employing random sampling techniques, but difficulties arise immediately at the next level of sophistication à la quantum state verification. One can mitigate this issue via conditional fidelities,^[115,27] but it remains an open question whether some nontrivial statements can be made about the full state produced by the source. A possible way out may be found in the de-Finetti reduction theorems,^[116] or with the help of entropy accumulation theorems,^[117,118] where resorting to permutational invariance is not allowed. Another option that may follow from our single-copy framework is to fold all accessible ((non-IID) copies setting into a large single-copy and perform verification in a single-copy scenario. While this seems to be a reasonable option, what remains to be clarified is: what is the class of states and properties that admit reliable single-copy verification/estimation? Our protocols reviewed here are the first steps towards answering this question. In this way, there is another conceptual issue to be addressed that concerns the operational meaning of physical quantities in a single-shot scenario.

A particularly pertinent open question, especially in the context of near term quantum devices is the trade-off between

measurement complexity and the corresponding increase or decrease of efficiently estimable quantities. As noted in refs. [22,29], the power of these techniques appears to be uniquely sourced from the choice of measurements performed. Specifically that they are two (in SQST) and three (in tomography) designs in t -design parlance.^[119] In particular, when estimators in classical shadow tomography are constructed from local measurements only, i.e., a one-design, the performance of the scheme drops significantly. Such a question was considered in the original work of classical shadows^[22] in the context of Pauli measurements, finding the complexity scaled unsurprisingly in the non-locality of the target observable. It also is something of the worst-case scenario in that one is restricted to a fixed set of weak measurements. Instead, one may introduce adaptability into the POVM implemented in the measurement phase of a scheme as was done by García-Pérez et al.^[120] Despite the optimization introducing increased classical post-processing into the protocol, it does not compromise the circuit complexity of the POVM. It remains less powerful than a complete shadow tomography but demonstrates high performance on the limited but highly relevant class of variational quantum eigensolver (VQE) problems.^[121]

This is a well-chosen compromise, since Clifford and MUB measurements are not trivial to implement owing to the inclusion of control operations between arbitrary subsystems, it is highly desirable to find similar reductions with perhaps different compromises being found for different problem instances. While certainly worth pursuing, this can be seen as equivalent to constructing POVMs that approximate a t -design of some order using a simpler set of generators than the Clifford group. Given that finding t -designs in the first place is already difficult, this is a challenging task.

With all these questions in mind, it appears that the time is nigh for an exciting new class of tomographic protocols, ones without the apparent drawbacks that have plagued state tomography since its inception allowing for direct probing of quantum systems in the NISQ technology regime and beyond.

Acknowledgements

J.M. and B.D. acknowledge support from the Austrian Science Fund (FWF) through BeyondC-F7112. V.S. acknowledges support from the FWF through BeyondC-F7113. A.G. acknowledges the funding provided by the Faculty of Physics, University of Belgrade, through the grant by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

few copies, quantum entanglement, quantum verification, state tomography

Received: September 1, 2021

Revised: December 21, 2021

Published online: March 17, 2022

- [1] J. Preskill, *Quantum* **2018**, *2*, 79.
- [2] J. Kelly, Z. Chen, B. Chiaro, B. Foxen, J. Martinis, Q. H. T. Team, *APS 2019*, 2019, A42.
- [3] N. Friis, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, B. Lanyon, *Phys. Rev. X* **2018**, *8*, 021012.
- [4] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, et al., *Science* **2020**, *370*, 1460.
- [5] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, et al., *Phys. Rev. Lett.* **2019**, *123*, 250503.
- [6] M. Gong, S. Wang, C. Zha, M.-C. Chen, H.-L. Huang, Y. Wu, Q. Zhu, Y. Zhao, S. Li, S. Guo, et al., *Science* **2021**, *372*, 948.
- [7] S. Ebadi, T. T. Wang, H. Levine, A. Keesling, G. Semeghini, A. Omran, D. Bluvstein, R. Samajdar, H. Pichler, W. W. Ho, et al., *Nature* **2021**, *595*, 227.
- [8] G. J. Mooney, G. A. White, C. D. Hill, L. C. Hollenberg, *Preprint arXiv:2102.11521* **2021**.
- [9] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al., *Nature* **2019**, *574*, 505.
- [10] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, et al., *Preprint arXiv:2106.14734* **2021**.
- [11] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, et al., *Preprint arXiv:2106.15534* **2021**.
- [12] D. F. James, P. G. Kwiat, W. J. Munro, A. G. White, in *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*, World Scientific, Singapore **2005**, pp. 509–538.
- [13] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, D. J. Wineland, *Phys. Rev. A* **2008**, *77*, 012307.
- [14] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, J. Eisert, *Phys. Rev. Lett.* **2010**, *105*, 150401.
- [15] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, I. Kerenidis, *Phys. Rev. Lett.* **2012**, *108*, 260502.
- [16] M. C. Tran, B. Dakić, F. Arnault, W. Laskowski, T. Paterek, *Phys. Rev. A* **2015**, *92*, 050301.
- [17] A. Montanaro, *Preprint arXiv:1707.04012* **2017**.
- [18] S. Pallister, N. Linden, A. Montanaro, *Phys. Rev. Lett.* **2018**, *120*, 170502.
- [19] G. Torlai, G. Mazzola, J. Carrasquilla, M. Troyer, R. Melko, G. Carleo, *Nat. Phys.* **2018**, *14*, 447.
- [20] H. Zhu, M. Hayashi, *Phys. Rev. Applied* **2019**, *12*, 054047.
- [21] M. Guță, J. Kahn, R. Kueng, J. A. Tropp, *J. Phys. A* **2020**, *53*, 204001.
- [22] H.-Y. Huang, R. Kueng, *Preprint arXiv:1908.08909* **2019**.
- [23] A. Dimić, B. Dakić, *NPJ Quantum Inf.* **2018**, *4*, 11.
- [24] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, *Nat. Phys.* **2019**, *15*, 935.
- [25] H.-Y. Huang, R. Kueng, J. Preskill, *Nat. Phys.* **2020**, *16*, 1050.
- [26] H. Zhu, M. Hayashi, *Phys. Rev. A* **2019**, *99*, 052346.
- [27] A. Dimić, I. Šupić, B. Dakić, *Preprint arXiv:2105.05832* **2021**.
- [28] S. Aaronson, *SIAM J. Comput.* **2019**, *49*, 5 STOC18.
- [29] J. Morris, B. Dakić, *Preprint arXiv:1909.05880* **2019**.
- [30] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, E. Kashefi, *Nat. Rev. Phys.* **2020**, *2*, 382.
- [31] S. T. Flammia, Y.-K. Liu, *Phys. Rev. Lett.* **2011**, *106*, 230501.
- [32] D. Hangleiter, *Preprint arXiv:2012.07905* **2020**.
- [33] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* **2009**, *81*, 865.
- [34] N. Friis, G. Vitagliano, M. Malik, M. Huber, *Nat. Rev. Phys.* **2019**, *1*, 72.
- [35] O. Gühne, G. Tóth, *Phys. Rep.* **2009**, *474*, 1.

- [36] B. M. Terhal, *Phys. Lett. A* **2000**, 271, 319.
- [37] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, A. Sanpera, *J. Mod. Opt.* **2002**, 49, 1399.
- [38] F. Baccari, D. Cavalcanti, P. Wittek, A. Acín, *Phys. Rev. X* **2017**, 7, 021042.
- [39] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, V. Scarani, *Phys. Rev. Lett.* **2011**, 107, 050502.
- [40] R. F. Werner, M. M. Wolf, *Preprint quant-ph/0107093* **2001**.
- [41] Y. Akbari-Kourbolagh, M. Azhdargalam, *Phys. Rev. A* **2019**, 99, 012304.
- [42] P. Hyllus, W. Laskowski, R. Krischek, C. Schwemmer, W. Wieczorek, H. Weinfurter, L. Pezzé, A. Smerzi, *Phys. Rev. A* **2012**, 85, 022321.
- [43] N. Li, S. Luo, *Phys. Rev. A* **2013**, 88, 014301.
- [44] Y.-Y. Zhao, G.-Y. Xiang, X.-M. Hu, B.-H. Liu, C.-F. Li, G.-C. Guo, R. Schwonnek, R. Wolf, *Phys. Rev. Lett.* **2019**, 122, 220401.
- [45] O. Gühne, N. Lütkenhaus, *Phys. Rev. Lett.* **2006**, 96, 170502.
- [46] J. C. Adcock, S. Morley-Short, J. W. Silverstone, M. G. Thompson, *Quantum Sci. Technol.* **2018**, 4, 015010.
- [47] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, et al., *Phys. Rev. Lett.* **2018**, 121, 250505.
- [48] A. Dimić, B. Dakić, *New J. Phys.* **2018**, 20, 063051.
- [49] O. Gühne, G. Tóth, H. J. Briegel, *New J. Phys.* **2005**, 7, 229.
- [50] H. J. Briegel, R. Raussendorf, *Phys. Rev. Lett.* **2001**, 86, 910.
- [51] M. R. Dowling, A. C. Doherty, S. D. Bartlett, *Phys. Rev. A* **2004**, 70, 062113.
- [52] D. Perez-Garcia, F. Verstraete, M. M. Wolf, J. I. Cirac, *Preprint quant-ph/0608197* **2006**.
- [53] F. Verstraete, V. Murg, J. I. Cirac, *Adv. Phys.* **2008**, 57, 143.
- [54] This example is rather explanatory and used to demonstrate the method. A “real” example of cluster states will naturally follow in the next section.
- [55] H. Chernoff, et al., *Ann. Math. Stat.* **1952**, 23, 493.
- [56] M. Hein, J. Eisert, H. J. Briegel, *Phys. Rev. A* **2004**, 69, 062311.
- [57] R. Raussendorf, H. J. Briegel, *Phys. Rev. Lett.* **2001**, 86, 5188.
- [58] L. Eldar, A. W. Harrow, in *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, **2017**, pp. 427–438.
- [59] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett. A* **2001**, 283, 1.
- [60] W. Laskowski, C. Schwemmer, D. Richart, L. Knips, T. Paterek, H. Weinfurter, *Phys. Rev. A* **2013**, 88, 022327.
- [61] L. Knips, C. Schwemmer, N. Klein, M. Wieśniak, H. Weinfurter, *Phys. Rev. Lett.* **2016**, 117, 210504.
- [62] Y. Chen, S. Ecker, J. Bavaresco, T. Scheidl, L. Chen, F. Steinlechner, M. Huber, R. Ursin, *Phys. Rev. A* **2020**, 101, 032302.
- [63] J. Bavaresco, N. H. Valencia, C. Klöckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, M. Huber, *Nat. Phys.* **2018**, 14, 1032.
- [64] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, A. Sanpera, *Phys. Rev. A* **2002**, 66, 062305.
- [65] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, J.-W. Pan, *Nat. Phys.* **2007**, 3, 91.
- [66] G. Tóth, O. Gühne, *Phys. Rev. Lett.* **2005**, 94, 060501.
- [67] V. Saggio, P. Walther, *Preprint arXiv:2201.02641* **2022**.
- [68] D. Browne, H. Briegel, *Quantum Information: From Foundations to Quantum Technology Applications*, Wiley-VCH, Weinheim **2016**, pp. 449–473.
- [69] G. Tóth, O. Gühne, *Phys. Rev. A* **2005**, 72, 022340.
- [70] M. Araújo, F. Hirsch, M. T. Quintino, *Quantum* **2020**, 4, 353.
- [71] M. Weilenmann, E. A. Aguilar, M. Navascues, *Preprint arXiv:2011.02216* **2020**.
- [72] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, G. Chen, C.-F. Li, G.-C. Guo, *Phys. Rev. Lett.* **2020**, 125, 030506.
- [73] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, et al., *Phys. Rev. Lett.* **2020**, 125, 030506.
- [74] Y.-C. Liu, J. Shang, R. Han, X. Zhang, *Phys. Rev. Lett.* **2021**, 126, 090504.
- [75] H. Zhu, M. Hayashi, *Phys. Rev. A* **2019**, 100, 062335.
- [76] H. Zhu, M. Hayashi, *Phys. Rev. Lett.* **2019**, 123, 260504.
- [77] Z. Li, Y.-G. Han, H. Zhu, *Phys. Rev. Appl.* **2020**, 13, 054002.
- [78] X.-D. Yu, J. Shang, O. Gühne, *NPJ Quantum Inf.* **2019**, 5, 1.
- [79] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, X. Zhang, *Phys. Rev. Appl.* **2019**, 12, 044020.
- [80] Y. Takeuchi, T. Morimae, *Phys. Rev. X* **2018**, 8, 021060.
- [81] X. Jiang, K. Wang, K. Qian, Z. Chen, Z. Chen, L. Lu, L. Xia, F. Song, S. Zhu, X. Ma, *NPJ Quantum Inf.* **2020**, 6, 90.
- [82] W.-H. Zhang, X. Liu, P. Yin, X.-X. Peng, G.-C. Li, X.-Y. Xu, S. Yu, Z.-B. Hou, Y.-J. Han, J.-S. Xu, et al., *NPJ Quantum Inf.* **2020**, 6, 1.
- [83] M. Hayashi, T. Morimae, *Phys. Rev. Lett.* **2015**, 115, 220502.
- [84] K. Fujii, M. Hayashi, *Physical Review A* **2017**, 96, 030301.
- [85] M. Hayashi, M. Hajdušek, *Phys. Rev. A* **2018**, 97, 052308.
- [86] D. Markham, A. Krause, *Cryptography* **2020**, 4, 3.
- [87] T. Morimae, K. Fujii, *Phys. Rev. A* **2013**, 87, 050301.
- [88] Y. Takeuchi, T. Morimae, M. Hayashi, *Sci. Rep.* **2019**, 9, 1.
- [89] S. Persegiers, G. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, A. Acín, *Rep. Prog. Phys.* **2013**, 76, 096001.
- [90] W. McCutcheon, A. Pappa, B. Bell, A. Mcmillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, et al., *Nat. Commun.* **2016**, 7, 1.
- [91] R. Colbeck, *Preprint arXiv:0911.3814* **2009**.
- [92] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., *Nature* **2010**, 464, 1021.
- [93] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, *Phys. Rev. Lett.* **2007**, 98, 230501.
- [94] V. Scarani, *Acta Phys. Slovaca* **2012**, 62, 347.
- [95] V. B. Braginsky, Y. I. Vorontsov, K. S. Thorne, *Science* **1980**, 209, 547.
- [96] G. Boole, *The Mathematical Analysis of Logic: Being an Essay Towards a Calculus of Deductive Reasoning*, Cambridge University Press, Cambridge **2009**.
- [97] T. Durt, B.-G. Englert, I. Bengtsson, K. Życzkowski, *Int. J. Quantum Inf.* **2010**, 08, 535.
- [98] I. D. Ivanovic, *J. Phys. A* **1981**, 14, 3241.
- [99] M. Wiesniak, T. Paterek, A. Zeilinger, *New J. Phys.* **2011**, 13, 053047.
- [100] J. Lawrence, i. c. v. Brukner, A. Zeilinger, *Phys. Rev. A* **2002**, 65, 032320.
- [101] O. Crawford, B. v. Straaten, D. Wang, T. Parks, E. Campbell, S. Brierley, *Quantum* **2021**, 5, 385.
- [102] S. Bernstein, *The Theory of Probabilities*, Gastehizdat Publishing House, London **1946**.
- [103] K. Dzhaparidze, J. van Zanten, *Stochastic Processes and their Applications*, North-Holland, Amsterdam **2001**.
- [104] M. Lerasle, *Preprint, arXiv:1908.10761* **2019**.
- [105] A. Klappenecker, M. Rötteler, *Proceedings. International Symposium on Information Theory*, 2005. (ISIT 2005.) **2005**, pp. 1740–1744.
- [106] C. Dankert, R. Cleve, J. Emerson, E. Livine, *Phys. Rev. A* **2009**, 80, 1.
- [107] J. Roik, K. Bartkiewicz, A. Černoch, K. Lemr, *Phys. Rev. Appl.* **2021**, 15, 054006.
- [108] M. Yosefpor, M. R. Mostaan, S. Raeisi, *Quantum Sci. Technol.* **2020**, 5, 045006.
- [109] Y. Chen, Y. Pan, G. Zhang, S. Cheng, *Preprint arXiv:2103.04804* **2021**.
- [110] G. M. D'Ariano, S. Mancini, V. I. Man'ko, P. Tombesi, *Quantum Semiclassical Opt.* **1996**, 8, 1017.
- [111] A. Gheorghiu, T. Kapourniotis, E. Kashefi, *Theor. Comput. Sys.* **2018**, 63, 715.
- [112] M. C. Tran, B. Dakić, F. m. c. Arnault, W. Laskowski, T. Paterek, *Phys. Rev. A* **2015**, 92, 050301.

- [113] M. C. Tran, B. Dakić, W. Laskowski, T. Paterek, *Phys. Rev. A* **2016**, *94*, 042302.
- [114] A. Ketterer, N. Wyderka, O. Gühne, *Phys. Rev. Lett.* **2019**, *122*, 120505.
- [115] J.-D. Bancal, K. Redecker, P. Sekatski, W. Rosenfeld, N. Sangouard, *Quantum* **2021**, *5*, 401.
- [116] M. Christandl, R. Renner, *Phys. Rev. Lett.* **2012**, *109*, 120403.
- [117] F. Dupuis, O. Fawzi, R. Renner, *Commun. Math. Phys.* **2020**, *379*, 867.
- [118] R. Arnon-Friedman, R. Renner, T. Vidick, *SIAM J. Comput.* **2019**, *48*, 181.
- [119] D. Gross, K. Audenaert, J. Eisert, *J. Math. Phys.* **2007**, *48*, 052104.
- [120] G. García-Pérez, M. A. C. Rossi, B. Sokolov, F. Tacchino, P. K. Barkoutsos, G. Mazzola, I. Tavernelli, S. Maniscalco, *Prx Quantum* **2021**, *2*, 040342.
- [121] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, J. L. O'brien, *Nat. Commun.* **2014**, *5*, 1.



Joshua Morris is a Ph.D. student at the University of Vienna, supervised by Dr Borivoje Dakić. His research primarily focuses on complexity in quantum systems, resource efficient tomography and semidefinite optimization.



Valeria Saggio received her Ph.D. in 2021 from the University of Vienna, under the supervision of Prof. Philip Walther. She is currently a postdoctoral associate at the Massachusetts Institute of Technology (MIT), USA. Her research focuses on experimental quantum optics and quantum computing with photonic platforms, from entanglement of many photons to quantum artificial intelligence.



Aleksandra Gočanin received her Ph.D. degree in physics from the University of Belgrade, Faculty of Physics under the supervision of Dr. Borivoje Dakić, in 2019. She is currently an assistant professor at the University of Belgrade, Faculty of Physics. Her research interests are resource-efficient ways of detecting quantum correlations, quantum state verification and foundations of quantum mechanics.



Borivoje Dakić is an assistant professor at the Faculty of Physics of the University of Vienna. His expertise lies in the quantum information theory, foundations of quantum mechanics and practical quantum information. He has made a significant contribution in the field of operational reconstructions of quantum theory, information-theoretic foundations of quantum correlations and interference phenomena, quantum verification theory and various theory-experimental research projects.