HAL
open science

Semi-device-independent characterization of multipartite entanglement of states and measurements

Armin Tavakoli, Alastair A. Abbott, Marc-Olivier Renou, Nicolas Gisin, Nicolas Brunner

To cite this version:

Armin Tavakoli, Alastair A. Abbott, Marc-Olivier Renou, Nicolas Gisin, Nicolas Brunner. Semi-device-independent characterization of multipartite entanglement of states and measurements. Physical Review A, 2018, 98 (5), pp.052333. 10.1103/PhysRevA.98.052333 . hal-02022606

HAL Id: hal-02022606

https://hal.science/hal-02022606v1

Submitted on 16 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Semi-device-independent characterisation of multipartite entangled states and measurements

Armin Tavakoli,[1] Alastair A. Abbott,[2] Marc-Olivier Renou,[1] Nicolas Gisin,[1] and Nicolas Brunner[1]

[1]*Département de Physique Appliquée, Université de Genève, CH-1211 Genève, Switzerland*
[2]*Univ. Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*

The semi-device-independent framework allows one to draw conclusions about properties of an unknown quantum system under weak assumptions. Here we present a semi-device-independent scheme for the characterisation of multipartite entanglement based around a game played by several isolated parties whose devices are uncharacterised beyond an assumption about the dimension of their Hilbert spaces. Our scheme can certify that an n-partite high-dimensional quantum state features genuine multipartite entanglement. Moreover, the scheme can certify that a joint measurement on n subsystems is entangled, and provides a lower bound on the number of entangled measurement operators. These tests are strongly robust to noise, and even optimal for certain classes of states and measurements, as we demonstrate with illustrative examples. Notably, our scheme allows for the certification of many entangled states admitting a local model, which therefore cannot violate any Bell inequality.

arXiv:1805.00377v1 [quant-ph] 1 May 2018

Introduction.—Entanglement represents a central feature of quantum theory and a key resource for quantum information processing [1]. Therefore, the task of characterising entanglement experimentally is of fundamental significance. In particular, the development of quantum networks, multiparty cryptography, quantum metrology, and quantum computing necessitate certification methods tailored to multipartite entangled states, as well as to entangled joint measurements.

Standard methods for the certification of multipartite entanglement rely on entanglement witnesses [2], as quantum tomography quickly becomes infeasible as the number of subsystems increases. Entanglement witnesses can also be used for the particularly important sub-case of certifying genuine multipartite entanglement (GME), the strongest form of multipartite entanglement, where all subsystems are genuinely entangled together; see, e.g., Refs. [1–3]. In practice, the main drawback of entanglement witnesses is that they crucially rely on the correct calibration of the measurement devices, as a set of specific observables must be measured. Importantly, even small alignment errors can have undesirable consequences, e.g. leading to false positives [4], and it is generally cumbersome to estimate these errors and take them into account rigorously.

This motivates the developments of certification methods that require minimal assumptions on the measurement devices, and in particular do not rely on their detailed characterisation. This is the spirit of the device-independent (DI) approach to entanglement characterisation, which also leads to interesting possibilities for quantum information processing [5–7]. The main idea consists in using Bell inequalities, given that a violation of such an inequality necessarily implies the presence of entanglement in the state (even without any knowledge about the measuring devices). Moreover, GME can also be detected via Bell-like inequalities [8–14]. Experimentally, however, this approach is very demanding as high visibilities are typically required. More generally, a broad range of entangled states (including many GME states [15–17]) cannot, in fact, violate any Bell inequality [18] as they admit local hidden variable models [19, 20]. Finally, although Bell inequalities can in principle be used for the certification of entangled joint measurements [21], no practical scheme has been reported thus far.

This motivates the exploration of partially DI scenarios, in between the fully DI case of Bell inequalities and the device-dependent case of entanglement witnesses. Here, only weak assumptions about the devices are typically made. One possibility is to consider that a subset of parties perform well-characterised measurements, while the others are uncharacterised [22–24]. Another option is to consider Bell experiments with quantum inputs, leading to the so-called measurement device-independent characterisation of entanglement [25, 26]. While experimental demonstrations have been reported, both of these approaches have the drawback of requiring certain parts of the experiment to be fully characterised.

In the present work, we follow a different approach for entanglement characterisation. Specifically, we will assume only an upper bound on the Hilbert space dimension of the subsystems of interest, but require no detailed characterisation of any of the devices. Roughly speaking, this assumption means that all the relevant degrees of freedom are described in a Hilbert space of given dimension [27–29], and that other potential side-channels can be neglected. This scenario, usually referred to as the semi-DI (SDI) setting, has been considered for the characterisation of entanglement in the simplest setting of two-qubit states [30, 31], as well as the detection of two-qubit entangled measurements [32, 33].

Here, we present a versatile scheme for characterising both multipartite entangled states and entangled measurements in a semi-DI setting. Our scheme allows one to simultaneously certify that (I) an n-partite quantum state (of arbitrary local dimension) is GME, and that (II) a measurement performed on the n subsystems is entangled. Furthermore, we obtain a finer characterisation for the measurement, namely a lower bound on the number of entangled measurement operators. In general our scheme is strongly robust to noise, and even optimal in certain cases. It certifies all noisy qubit Greenberger-Horne-Zeilinger (GHZ) states that are GME, and, in the bipartite case, all entangled isotropic states of arbitrary dimension. Other classes of GME states, e.g. Dicke states, can also be certified, although not optimally. For the case of entangled measurements, we give two illustrative examples. In particular, we optimally certify the presence of entanglement in a noisy Bell-state measurement. Finally, we conclude with a

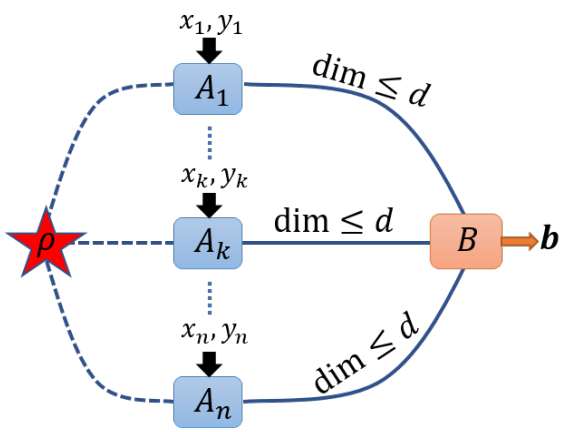

FIG. 1. An n-partite state is distributed between parties $A_1, \ldots, A_n$ who perform transformations on their local systems depending on their random inputs (x_k, y_k). Each party sends their transformed d-dimensional system to B who performs a measurement and obtains an outcome $\mathbf{b}$.

list of open questions.

Scenario.—The scenario we consider consists of a state being initially prepared, then transformed by several parties, and finally measured. Since we operate within the SDI framework no assumptions are made on the internal workings of any of these parties' devices, other than a bound on their local Hilbert space dimensions, see Fig. 1. Throughout the experiment the parties cannot communicate amongst themselves; one may consider, e.g., that they are spacelike separated as is usual in the DI framework.

Let an uncharacterised source distribute a state ρ of arbitrary dimension between n parties $A_1, \ldots, A_n$, each of which receives a subsystem. Each party A_k, for $k = 1, \ldots, n$, receives uniformly random inputs $x_k, y_k \in \{0, \ldots, d-1\}$. Subsequently, they perform local transformations $\mathcal{T}^{(k)}_{x_k y_k}$ (which may be any completely positive trace-preserving (CPTP) map) which map their local states into a d-dimensional state. The transformed state is sent to a final party denoted by B who performs a (possibly joint) measurement $\{M_\mathbf{b}\}_\mathbf{b}$ (i.e., a positive-operator valued measure (POVM) with $M_\mathbf{b} \geq 0$ and $\sum_\mathbf{b} M_\mathbf{b} = \mathbb{1}$) which produces an outcome string $\mathbf{b} = b_1 \ldots b_n \in \{0, \ldots, d-1\}^n$ (see Fig. 1). The experiment gives rise to a probability distribution $P(\mathbf{b}|\mathbf{x}, \mathbf{y})$, where $\mathbf{x} = x_1 \ldots x_n$ and $\mathbf{y} = y_1 \ldots y_n$, given by

$$P(\mathbf{b}|\mathbf{x}, \mathbf{y}) = \mathrm{tr}\left[\left(\bigotimes_{k=1}^{n} \mathcal{T}^{(k)}_{x_k y_k}\right)[\rho] \cdot M_\mathbf{b}\right]. \tag{1}$$

The goal of the task (or game) we consider is for the parties to cooperate so that B's output satisfies the conditions

$$b_1 = \sum_{i=1}^{n} x_i \equiv C_1(x) \quad \text{and} \quad b_k = y_k - y_1 \equiv C_k(y), \tag{2}$$

for $k = 2, \ldots, n$, where all quantities are computed modulo d. Compactly, we write $C(\mathbf{x}, \mathbf{y})$ for the (unique) string $\mathbf{b}$ satisfying all the above conditions. Note that these conditions are not totally symmetric (except when $n = 2$), but they will nonetheless prove useful in certifying entanglement. Given a strategy leading to a probability distribution $P(\mathbf{b}|\mathbf{x}, \mathbf{y})$, the probability of winning the task (or if a win is rewarded with a point, the average score) is thus given by

$$\mathcal{A}_{n,d} = \frac{1}{d^{2n}} \sum_{\mathbf{x},\mathbf{y}} P\left(\mathbf{b} = C(\mathbf{x}, \mathbf{y}) \,|\, \mathbf{x}, \mathbf{y}\right). \tag{3}$$

We now show how, from the value of an observed average score $\mathcal{A}_{n,d}$, one can make inferences about the entanglement of the state ρ and the measurement $\{M_\mathbf{b}\}_\mathbf{b}$.

Characterising entangled states.—We first consider certifying the GME of the shared state. A state is said to be GME if it is not biseparable, i.e., if it cannot be written in the form $\rho = \sum_S \sum_i p_{S,i} \rho_i^S \otimes \rho_i^{\bar{S}}$, for any possible bipartition $\{S, \bar{S}\}$ of the subsystems $\{1, \ldots, n\}$, where $\sum_{S,i} p_{S,i} = 1$ and $p_{S,i} \geq 0$.

We now show that the value of $\mathcal{A}_{n,d}$ can be nontrivially upper bounded for any n-partite biseparable state. This will allow us to certify GME since, as we will see later, the bound is violated by many GME states of interest.

Result 1. *Let ρ be a state of n subsystems. For any measurement $\{M_\mathbf{b}\}_\mathbf{b}$ and any transformations $\{\mathcal{T}^{(k)}_{x_k y_k}\}_k$, it holds that*

$$\rho \text{ is biseparable} \implies \mathcal{A}_{n,d} \leq 1/d. \tag{4}$$

Hence, whenever $\mathcal{A}_{n,d} > 1/d$, ρ is certified to be GME. Moreover, this inequality is tight and the bound can be saturated with fully separable states.

Proof. The full details of the proof are given in Appendix A. In order to prove the upper bound in (4), we consider a relaxed SDI task in which any distribution $P(\mathbf{b}|\mathbf{x}, \mathbf{y})$ obtainable in the original task is also possible in the relaxed setting, but not vice versa. The relaxation is chosen so that the average score $\mathcal{A}_{n,d}$ can easily be upper-bounded. By construction, the upper bound obtained in the relaxed scenario is also valid for the original task.

To see that the bound is tight, we give a strategy that utilises only product states and saturates the bound (4). Let A_k (for $k = 1, \ldots, n$) send y_k to party B. With this information, B can output $b_i = y_i - y_1$, satisfying condition C_i, for $i = 2, \ldots, n$. However, this strategy forces B to guess b_1 in order to satisfy condition C_1. Any such guess succeeds, on average, with probability $1/d$, thus saturating the bound. □

In order to show the relevance of the relation in Eq. (4), we show that it can be violated by GME states. In particular, we first consider the largest achievable value of $\mathcal{A}_{n,d}$. It turns out that the algebraically maximal value, i.e., $\mathcal{A}_{n,d} = 1$, can be achieved for all n and d via the following strategy. A GME state of n subsystems of local dimension d, namely the generalised GHZ state,

$$|\mathrm{GHZ}_{n,d}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes n} \tag{5}$$

is distributed among the parties $A_1, \ldots, A_n$. Each party then performs the unitary transformation $U^{A_k}_{x_k y_k} = Z^{x_k} X^{y_k}$ for $k = 1, \ldots, n$, where

$$Z = \sum_{j=0}^{d-1} e^{2i\pi j/d} |j\rangle\langle j|\,, \quad X = \sum_{j=0}^{d-1} |j+1\rangle\langle j| \tag{6}$$

are the usual clock and shift operators. Finally, B performs a joint projective measurement in the basis of generalised GHZ states given by

$$|M_b\rangle = Z^{b_1} \otimes X^{b_2} \otimes \cdots \otimes X^{b_n} |\mathrm{GHZ}_{n,d}\rangle. \tag{7}$$

Note that in the simplest case of two qubits ($n = d = 2$), the four unitaries are simply the three Pauli matrices and the identity matrix, while the measurement is the Bell-state measurement [34].

Let us now consider noisy GHZ states, i.e., mixtures of GHZ states with white noise: $\rho^{\mathrm{GHZ}}_{n,d}(v) = v\,|\mathrm{GHZ}_{n,d}\rangle\langle\mathrm{GHZ}_{n,d}| + (1-v)\mathbb{1}/d^n$, where $v \in [0,1]$ is the visibility of the state. In the strategy given above, for the white noise state one has $\mathcal{A}_{n,d}(\mathbb{1}/d^n) = 1/d^n$. Hence, from the linearity of $\mathcal{A}_{n,d}$ in ρ, it follows that a violation of Eq. (4) is obtained whenever $v + (1-v)/d^n > 1/d$, that is, when $v > (d^{n-1}-1)/(d^n-1)$. We discuss the implications of this result in three separate cases of interest.

(I) For two d-dimensional systems ($n = 2$), the criterion is $v > 1/(d+1)$ which is precisely the condition for the entanglement of $\rho^{\mathrm{GHZ}}_{2,d}(v)$ [35]. Hence, every entangled isotropic bipartite state is certified by our protocol. Interestingly, such certification is impossible using Bell inequalities; for instance we note that the state $\rho^{\mathrm{GHZ}}_{2,2}(v)$ has a local hidden variable model (for projective measurements) when $v < 0.6829$ [36], and will therefore not violate any (known or unknown) Bell inequality. For large d, such models are known for $v \leq \log d/d$ [37], and, in the limit, known facet Bell inequalities allow for the certification of $\rho^{\mathrm{GHZ}}_{2,d}(v)$ when $v > 0.67$ [38]. In contrast, as $d \to \infty$ our protocol can certify entanglement for arbitrary small v.

(II) In the case of a system of many qubits ($d = 2$), our visibility criterion coincides with the condition for $\rho^{\mathrm{GHZ}}_{n,2}(v)$ to be GME [39]. Hence our scheme can certify all noisy qubit GHZ states that are GME. Again, this would not be possible using Bell inequalities, as (for instance) the state $\rho^{\mathrm{GHZ}}_{3,2}(v = 1/2)$ is GME but admits a biseparable model reproducing all correlations from projective measurements [10]. Furthermore, the GME of $\rho^{\mathrm{GHZ}}_{3,2}(v)$ is known to be certifiable via a Bell inequality (in the limit of many measurements) when $v > 0.64$ [11], whereas our criterion reads $v > 3/7$.

(III) When considering many high-dimensional systems ($n > 2$ and $d > 2$), our setup is no longer optimal since there exist generalised GHZ states that are GME below the critical visibility of our scheme [40]. Nevertheless, choosing, for instance, $n = d = 3$, the criterion is $v > 4/13$ which substantially outperforms the certification obtainable via known Bell inequalities, which is possible when $v > 0.81$ [10, 14].

More generally, we derive a lower bound on the maximal value of $\mathcal{A}_{n,d}$ achievable for an arbitrary state ρ. To this end, consider the following strategy. Let B perform the measurement given by (7), and let each party A_k perform the transformation $\mathcal{T}^{(k)}_{x_k y_k}[\rho] = (U^{A_k}_{x_k y_k})\,\Lambda_k[\rho]\,(U^{A_k}_{x_k y_k})^\dagger$, where $U^{A_k}_{x_k y_k} = Z^{x_k} X^{y_k}$ and the Λ_k, for $k = 1, \ldots, n$, are CPTP maps. Evaluating the score with this strategy and optimising over the CPTP maps $\Lambda_1, \ldots, \Lambda_n$ straightforwardly leads to

$$\mathcal{A}_{n,d}(\rho) = \mathrm{EGF}_{n,d}(\rho), \tag{8}$$

where we have defined the quantity $\mathrm{EGF}_{n,d}(\rho) = \max_{\Lambda_1,\ldots,\Lambda_n} \mathrm{tr}\left[(\bigotimes_{k=1}^n \Lambda_i)[\rho] \cdot |\mathrm{GHZ}_{n,d}\rangle\langle\mathrm{GHZ}_{n,d}|\right]$. If one instead maximises only over unitary maps $\Lambda_k[\rho] = V_k \rho V_k^\dagger$ one obtains $A_{n,d} = \mathrm{GF}_{n,d}(\rho)$, where $\mathrm{GF}_{n,d}(\rho) = \max_{V_1,\ldots,V_n} \mathrm{tr}\left[(\bigotimes_{k=1}^n V_i)\,\rho\,(\bigotimes_{k=1}^n V_i)^\dagger |\mathrm{GHZ}_{n,d}\rangle\langle\mathrm{GHZ}_{n,d}|\right]$ is the *GHZ fraction* [41], a multipartite generalisation of the singlet fraction [35]. $\mathrm{EGF}_{n,d}(\rho)$ can then be seen as the "extractable" GHZ fraction, an important generalisation since, even in the bipartite case, local CPTP maps can increase the singlet fraction of an entangled state [42].

In order to determine whether one can obtain a better score than that given by Eq. (8) by considering arbitrary transformations and measurements, we conducted extensive numerical tests. Focusing on the cases $(n,d) \in \{(2,2),(2,3),(3,2)\}$ and optimising numerically $\mathcal{A}_{n,d}$ starting from randomly chosen transformations and measurements, we were unable to obtain a better score than $\mathrm{EGF}_{n,d}(\rho)$. We note also that, when restricted to unitary transformations, we were similarly unable to obtain a score larger than $\mathrm{GF}_{n,d}(\rho)$. Motivated by this numerical evidence, we make the following conjecture:

Conjecture 1. *Let ρ be an n-partite state of local dimension d. Then the maximal value of $\mathcal{A}_{n,d}$ achievable for any measurement $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ and transformations $\{\mathcal{T}^{(k)}_{x_k y_k}\}_k$ is $\mathrm{EGF}_{n,d}(\rho)$, i.e.,*

$$\max_{\{\mathcal{T}^{(k)}_{x_k y_k}\},\{M_{\mathbf{b}}\}_{\mathbf{b}}} \mathcal{A}_{n,d}(\rho) = \mathrm{EGF}_{n,d}(\rho). \tag{9}$$

Proving this conjecture would be particularly interesting in the bipartite case, as violation of our witness would then certify an extractable singlet fraction greater than $1/d$, which implies that maximal entanglement can be distilled from the state ρ [35].

We conclude this part, by discussing other classes of GME states, that are qualitatively inequivalent to GHZ states. Let us first consider noisy W states of three qubits, i.e., $W(v) = v\,|W\rangle\langle W| + (1-v)\mathbb{1}/8$, where $|W\rangle = \frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big)$. Numerical optimisation gives a (seemingly optimal) strategy obtaining $\mathcal{A}_{3,2} = \frac{1}{8}(1+5v)$. This implies that our scheme certifies the GME of $W(v)$ for $v > 3/5$. This is relatively close to the optimal visibility for GME of $v > 0.48$ [43]. In comparison, known DI schemes based on Bell inequalities would require $v > 0.72$ [10].

As a second illustrative example, we consider a noisy four-qubit Dicke state $D(v) = v\,|D\rangle\langle D| + (1-v)\mathbb{1}/16$, where $|D\rangle = \frac{1}{\sqrt{6}}\big(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle\big)$. Numerically, the best strategy we find certifies the GME of $D(v)$ for $v > 7/11 \approx 0.64$, while it is known to be GME for $v > 0.46$ [43].

Characterising entangled measurements.—Next, we consider characterising the entanglement of the joint measurement performed by B. A measurement $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ is said to be entangled if at least one measurement operator $M_{\mathbf{b}}$ does not have a fully separable decomposition $M_{\mathbf{b}} = \sum_i M_{\mathbf{b},i}$ where $M_{\mathbf{b},i} \geq 0$ and each $M_{\mathbf{b},i}$ has the tensor product form $M_{\mathbf{b},i} = \bigotimes_{k=1}^n M_{\mathbf{b},i}^{(k)}$. We will see that the separability of $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ imposes a nontrivial bound on $\mathcal{A}_{n,d}$ which will allow us to certify the entanglement of the measurement used. However, it is sufficient for a single measurement operator to be entangled in order for the measurement to be entangled. This qualitative property rules out a classical description, but reveals little about the extent to which entanglement is present in the measurement. Interestingly, we can go a step further and show that the value of $\mathcal{A}_{n,d}$ implies a bound on the minimum number of the d^n measurement operators that are entangled. This provides a much finer characterisation of the joint entangled measurement performed by B.

Result 2. *Let $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ be a joint measurement of an n-partite system of local dimension d with at least $k \in \{0, \ldots, d^n\}$ fully separable measurement operators. For any n-partite state ρ and any transformations $\{\mathcal{T}_{x_k y_k}^{(k)}\}_k$ it holds that*

$$\text{At least } k \text{ separable measurement operators} \implies \mathcal{A}_{n,d} \leq \frac{1}{d^n}\left(d^n - k + \frac{k}{d}\right). \quad (10)$$

Hence, a violation of this inequality for a particular k implies that at least $d^n - k + 1$ measurement operators are entangled.

Proof. The proof is given in Appendix B. □

In the extremal case of a fully separable measurement ($k = d^n$), the bound (10) reduces to $\mathcal{A}_{n,d} \leq 1/d$, and observing a violation of this bound certifies the entanglement of the measurement. In the other extreme of witnessing a measurement whose operators are all entangled (i.e., violating Eq. (10) for $k = 1$), the bound (10) is $\mathcal{A}_{n,d} \leq 1 - (d-1)/d^{n+1}$, which is nontrivial for all n and d. In Appendix C we give some partial results on the tightness of Eq. (10).

To demonstrate the usefulness of Result 2, we now discuss two illustrative examples in the bipartite case. First we consider a noisy version of a generalised Bell-state measurement (for arbitrary d), which, we recall, is a joint measurement of two d-level systems given by the projection onto a basis of d^2 maximally entangled states $\{|M_{b_1 b_2}\rangle\}_{b_1 b_2}$. To this end, we consider the measurement operators $M_{b_1 b_2}(v) = v\,|M_{b_1 b_2}\rangle\langle M_{b_1 b_2}| + (1-v)\mathbb{1}/d^2$. Note that each of these measurement operators is equivalent (up to local unitaries) to an isotropic state $\rho_{2,d}^{\text{GHZ}}(v)$, and is thus entangled precisely when $v > 1/(d+1)$.

To certify the entanglement of this measurement, consider again the strategy used previously in which the parties share a maximally entangled state of two d-level systems, and perform the unitary transformations $U_{x_k y_k}^{A_k} = Z^{x_k} X^{y_k}$. Note that the score obtained here is the same as when considering a shared noisy isotropic state $\rho_{2,d}^{\text{GHZ}}(v)$, combined with an ideal Bell-state measurement. It thus follows from the previous results that we can certify the entanglement of the measurement whenever $v > 1/(d+1)$. Hence, we certify entanglement whenever the level of noise is low enough to keep the measurement operators entangled. Nevertheless, note that in this case our witness certifies only that at least one measurement operator is entangled, while all the measurement operators are in fact entangled. In order to certify the entanglement of all d^2 measurement operators, a much higher visibility of $v > (d^2+d-1)/(d^2+d)$ is required. In the simplest case of qubits ($d = 2$) this requirement is $v > 5/6$.

The second example we consider is for the case $n = d = 2$, where we look at a two-qubit Bell-state measurement subjected to coloured noise. Defining the usual Bell basis $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, and $\Phi^\pm = |\phi^\pm\rangle\langle\phi^\pm|$, $\Psi^\pm = |\psi^\pm\rangle\langle\psi^\pm|$, consider the measurement given by the operators

$$E_{00} = v\Phi^+ + \frac{1-v}{4}\left(\Phi^+ + 2\Phi^- + \Psi^+\right) \quad (11)$$

$$E_{01} = v\Psi^+ + \frac{1-v}{4}\left(\Phi^+ + \Phi^- + 2\Psi^+\right) \quad (12)$$

$$E_{10} = v\Phi^- + \frac{1-v}{4}\left(2\Phi^+ + \Phi^- + \Psi^+\right) \quad (13)$$

$$E_{11} = \Psi^-, \quad (14)$$

for some visibility $v \in [0,1]$. When $1/3 < v \leq 1$, all four operators are entangled; when $0 < v \leq 1/3$, only E_{01} and E_{11} are entangled; and when $v = 0$, only E_{11} is entangled.

Considering the same strategy as in the previous example (i.e., sharing a maximally entangled state and applying the transformations $U_{x_k y_k}^{A_k}$), we find $\mathcal{A}_{2,2} = (1+v)/2$. By virtue of Eq. (10), this certifies the presence of four entangled measurement operators when $v > 3/4$, at least three when $v > 1/2$, at least two when $v > 1/4$, and at least one when $v > 0$.

Conclusion.—We presented a scheme for the semi-device-independent characterisation of multipartite entangled states and measurements. In particular, our scheme can both certify that states are GME, and provide a lower bound on the number of measurement operators that are entangled. We illustrated the relevance of our scheme in various case studies, showing strong robustness to noise. In particular, we showed that at the price of a dimensional bound, one can overcome fundamental limitations of entanglement certification using Bell inequalities, as our scheme can certify many entangled states admitting a local model.

We conclude with some relevant open questions. (I) Does Eq. (10) hold also for biseparable (rather than fully separable) measurement operators, thereby allowing the number of GME measurement operators to be bounded? (II) Can a more sophisticated semi-DI scheme certify the entanglement of all GME states (not just particular classes of states, as shown here)? (III) Can our scheme be used as a dimension witness for both states and measurements (e.g., obtaining a score $\mathcal{A}_{n,d} = 1$ seems to require a state and measurement of dimension at least d^n)? (IV) Note that a score $\mathcal{A}_{n,d} = 1$ implies that all the relations (2) are satisfied. This makes the scheme a good candidate for multiparty cryptographic tasks (e.g., secret sharing of classical data with quantum resources). Exploring this possibility would be interesting. (V) Can the scheme

be used for self-testing states, measurements, and transformations in prepare-and-measure experiments [44]?

Acknowledgements.—We thank Cyril Branciard for discussions. This work was supported by the Swiss national science foundation (Starting grant DIAQ, NCCR-QSIT) and the French National Research Agency (Retour Post-Doctorants programme grant ANR-13-PDOC-0026).

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865 (2009).

[2] O. Gühne and G. Toth, "Entanglement detection," Phys. Rep. **474**, 1 (2009).

[3] C. Eltschka and J. Siewert, "Quantifying entanglement resources," J. Phys. A **47**, 424005 (2014).

[4] D. Rosset, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin, and Y.-C. Liang, "Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses," Phys. Rev. A **86**, 062325 (2012).

[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).

[6] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis, University of Cambridge (2006), arXiv:0911.3814 [quant-ph].

[7] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021 (2010).

[8] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, "Bell-type inequalities to detect true n-body nonseparability," Phys. Rev. Lett. **88**, 170405 (2002).

[9] M. Seevinck and G. Svetlichny, "Bell-type inequalities for partial separability in n-particle systems and quantum mechanical violations," Phys. Rev. Lett. **89**, 060401 (2002).

[10] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, "Device-independent witnesses of genuine multipartite entanglement," Phys. Rev. Lett. **106**, 250404 (2011).

[11] K. F. Pál and T. Vértesi, "Multisetting Bell-type inequalities for detecting genuine multipartite entanglement," Phys. Rev. A **83**, 062123 (2011).

[12] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang, "A framework for the study of symmetric full-correlation Bell-like inequalities," J. Phys. A **45**, 125301 (2012).

[13] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, "Device-independent entanglement quantification and related applications," Phys. Rev. Lett. **111**, 030501 (2013).

[14] G. Murta, R. Ramanathan, N. Móller, and M. Terra Cunha, "Quantum bounds on multiplayer linear games and device-independent witness of genuine tripartite entanglement," Phys. Rev. A **93**, 022305 (2016).

[15] G. Tóth and A. Acín, "Genuine tripartite entangled states with a local hidden-variable model," Phys. Rev. A **74**, 030306 (2006).

[16] R. Augusiak, M. Demianowicz, J. Tura, and A. Acín, "Entanglement and nonlocality are inequivalent for any number of parties," Phys. Rev. Lett. **115**, 030404 (2015).

[17] J. Bowles, J. Francfort, M. Fillettaz, F. Hirsch, and N. Brunner, "Genuinely multipartite entangled quantum states with fully local hidden variable models and hidden multipartite nonlocality," Phys. Rev. Lett. **116**, 130401 (2016).

[18] Note that nonlocality can nevertheless be activated in some more sophisticated Bell scenarios involving, e.g., sequential measurements [45] or processing of multiple copies [46]. Furthermore, with the help of additional sources of perfect singlets, any entangled bipartite state can be certified [47].

[19] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Phys. Rev. A **40**, 4277 (1989).

[20] R. Augusiak, M. Demianowicz, and A. Acín, "Local hidden variable models for entangled quantum states," J. Phys. A **42**, 424002 (2014).

[21] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, and V. Scarani, "Device-independent certification of entangled measurements," Phys. Rev. Lett. **107**, 050502 (2011).

[22] Q. Y. He and M. D. Reid, "Genuine multipartite Einstein-Podolsky-Rosen steering," Phys. Rev. Lett. **111**, 250403 (2013).

[23] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn, "Detection of entanglement in asymmetric quantum networks and multipartite quantum steering," Nat. Commun. **6**, 7941 (2015).

[24] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, "Experimental verification of multipartite entanglement in quantum networks," Nat. Commun. **7**, 13251 (2016).

[25] F. Buscemi, "All entangled quantum states are nonlocal," Phys. Rev. Lett. **108**, 200401 (2012).

[26] C. Branciard, D. Rosset, Y-C. Liang, and N. Gisin, "Measurement-device-independent entanglement witnesses for all entangled quantum states," Phys. Rev. Lett. **110**, 060405 (2013).

[27] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," Phys. Rev. A **84**, 010302 (2011).

[28] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Semi-device-independent randomness certification using $n \to 1$ quantum random access codes," Phys. Rev. A **85**, 052308 (2012).

[29] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, "Quantum random access codes using single d-level systems," Phys. Rev. Lett. **114**, 170502 (2015).

[30] Y.-C. Liang, T. Vértesi, and N. Brunner, "Semi-device-independent bounds on entanglement," Phys. Rev. A **83**, 022108 (2011).

[31] K. T. Goh, J.-D. Bancal, and V. Scarani, "Measurement-device-independent quantification of entanglement for given Hilbert space dimension," New J. Phys. **18**, 045022 (2016).

[32] T. Vértesi and M. Navascués, "Certifying entangled measurements in known Hilbert spaces," Phys. Rev. A **83**, 062112 (2011).

[33] A. Bennet, T. Vértesi, D. J. Saunders, N. Brunner, and G. J. Pryde, "Experimental semi-device-independent certification of entangled measurements," Phys. Rev. Lett. **113**, 080405 (2014).

[34] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895 (1993).

[35] M. Horodecki, P. Horodecki, and R. Horodecki, "General teleportation channel, singlet fraction, and quasidistillation," Phys. Rev. A **60**, 1888 (1999).

[36] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, "Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$," Quantum **1**, 3 (2017).

[37] M. L. Almeida, S. Pironio, J. Barrett, G. Tóth, and A. Acín, "Noise robustness of the nonlocality of entangled quantum states," Phys. Rev. Lett. **99**, 040403 (2007).

[38] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, "Bell inequalities for arbitrarily high-dimensional systems," Phys. Rev. Lett. **88**, 040404 (2002).

[39] S. M. Hashemi Rafsanjani, M. Huber, C. J. Broadbent, and J. H. Eberly, "Genuinely multipartite concurrence of N-qubit X-matrices," Phys. Rev. A **86**, 062303 (2012).

[40] F. Clivaz, M. Huber, L. Lami, and G. Murta, "Genuine-multipartite entanglement criteria based on positive maps," J. Math. Phys. **58**, 082201 (2017).

[41] J. Xu, "Multipartite fully entangled fraction," Int. J. Theor. Phys. **55**, 2904 (2016).

[42] P. Horodecki P. Badziag, M. Horodecki and R. Horodecki, "Local environment can enhance fidelity of quantum teleportation," Phys. Rev. A **62**, 012311 (2000).

[43] B. Jungnitsch, T. Moroder, and O. Gühne, "Taming multiparticle entanglement," Phys. Rev. Lett. **106**, 190502 (2011).

[44] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, "Self-testing quantum states and measurements in the prepare-and-measure scenario," arXiv:1801.08520 [quant-ph].

[45] S. Popescu, "Bell's inequalities and density matrices: Revealing "hidden" nonlocality," Phys. Rev. Lett. **74**, 2619–2622 (1995).

[46] C. Palazuelos, "Superactivation of quantum nonlocality," Phys. Rev. Lett. **109**, 190401 (2012).

[47] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, "Device-independent entanglement certification of all entangled states," arXiv:1801.10444 [quant-ph].

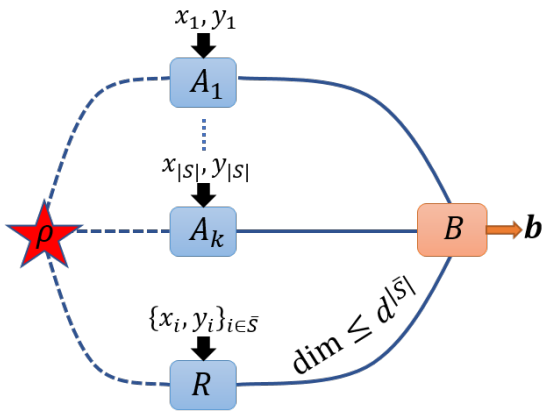

FIG. 2. The modified scenario (cf. Fig. 1). Parties $\{A_k\}_{k\in S}$ are allowed unlimited communication to B, whereas the remaining parties $\{A_k\}_{k\in\bar{S}}$ are grouped into a single party, R, allowed $\bar{S}\log d$ bits of communication. The case shown is for $S = \{1, \ldots, |S|\}$.

Appendix A: Proof of Result 1

In this section, we prove Result 1. Specifically, we bound the maximal value of $\mathcal{A}_{n,d}$ that can be obtained by biseparable states, regardless of the choice of transformations and measurements. Since $\mathcal{A}_{n,d}$ depends linearly on ρ, no mixed biseparable state can be used to obtain a larger score than some pure biseparable state. Hence, we need only consider pure states of the form $|\chi\rangle_S \equiv |\psi\rangle_S \otimes |\phi\rangle_{\bar{S}}$, for any nontrivial bipartition $\{S, \bar{S}\}$ of the set of subsystems $\{1, \ldots, n\}$.

Consider $|\chi\rangle_S$ for a particular bipartition $\{S, \bar{S}\}$. In order to give an upper bound on $\mathcal{A}_{n,d}$, we will relax some of the constraints in the scenario considered by the scheme and then evaluate the maximal average score in this less restrictive setting. In particular, we consider the scenario in which the parties $\{A_k\}_{k\in S}$ are permitted to communicate unbounded information to B, while the remaining parties $\{A_k\}_{k\in\bar{S}}$ are grouped into a single "effective" party R, and which receives all their inputs. The party R is allowed to send $|\bar{S}|$ d-level quantum systems (equivalently, a system of dimension $d^{|\bar{S}|}$) to B. This scenario is illustrated in Fig. 2.

It is clear that any probability distribution $P(\mathbf{b}|\mathbf{x}, \mathbf{y})$ obtainable in the original scenario on a state $|\chi\rangle_S$ (i.e., with some choice of transformations and measurements), is also obtainable in the relaxed scenario, but not vice versa. Since, by assumption, there is no entanglement over the bipartition $\{S, \bar{S}\}$, the parties $\{A_k\}_{k\in S}$ cannot do better than to simply send all their inputs to B. In order to win the game, R therefore needs to communicate to B the values of $\sum_{i\in\bar{S}} x_i$ and all $\{y_i\}_{i\in\bar{S}}$ for the conditions $C_1, \ldots, C_n$ to be satisfied. However, this amounts to $\left(|\bar{S}| + 1\right)\log d$ bits of information, while R can generally only send $|\bar{S}|\log d$ bits using a $d^{|\bar{S}|}$-level system, and must therefore employ a nontrivial optimal communication strategy. As we demonstrate more formally below, there is no quantum strategy that allows B to know this information with a probability higher than $1/d$, and therefore cannot with the game with a probability better than this either. Consequently, the desired bound in Eq. (4) follows.

To this end, let us consider the following general setting for an information compression task between two parties, Alice and Bob. Let Alice receive a uniformly distributed input $x \in \{1, \ldots, N\}$ which she must communicate to Bob. She encodes this input into a quantum state ρ_x of dimension at most d, with $N > d$ (if $N \leq d$ then Alice can simply send x). This amounts to Alice compressing her input into a smaller message to send. This message is then sent to Bob, who must attempt to retrieve the value of x from the state ρ_x by performing a suitable measurement $\{M_b\}_{b=1}^N$. What is the average probability of success for Bob to correctly obtain x following this measurement? A quantum strategy must obey the following bound:

$$p^{\text{success}} \equiv \frac{1}{N}\sum_{x=1}^{N} P^{\text{Q}}(b = x|x) = \frac{1}{N}\sum_{x=1}^{N} \text{tr}\left(\rho_x M_x\right) \leq \frac{1}{N}\sum_{x=1}^{N} \lambda_{\text{max}}\left(M_x\right) \leq \frac{1}{N}\sum_{x=1}^{N} \text{tr}\left(M_x\right) = \frac{1}{N}\,\text{tr}\left(\sum_{x=1}^{N} M_x\right) = \frac{d}{N}, \quad \text{(A1)}$$

where we have used the fact that the optimal state ρ_x maximising $\text{tr}(\rho_x M_x)$ is the eigenvector of M_x corresponding to its largest eigenvalue, and that $\lambda_{\text{max}}(M_x) \leq \text{tr}\left(M_x\right)$. In the last step we used that $\sum_x M_x = \mathbb{1}_d$ for any POVM $\{M_x\}_x$.

Moreover, there is no quantum advantage over classical approaches to encode and decode this information. This is straightforwardly seen by noting that the quantum bound (A1) can be saturated with a classical strategy as follows. Let Alice send the classical message $m(x) = x$ whenever $x = 1, \ldots, d$, and $m(x) = d$ if $x \in \{d+1, \ldots, N\}$. Bob always outputs the message he receives, i.e. $b = m(x)$. Whenever $x \in \{1, \ldots, d\}$, it is indeed true that $b = x$ and Bob correctly obtains x; when

$x \in \{d+1, \ldots, N\}$, Bob never succeeds. The average success probability of this simple classical strategy reads

$$p^{\text{success}} \equiv \frac{1}{N} \sum_{x=1}^{N} P^{\text{C}}(b = x|x) = \frac{d}{N}. \tag{A2}$$

Hence, quantum theory provides no advantage over classical coding for the stated task. Note that the above bears resemblance to the Holevo bound, with the difference that we are probabilistically accessing the information.

We can now apply this result to the relaxed scenario under consideration in the proof of Result 1. There, the effective party R plays the role of Alice, and has to transmit to Bob which of the $d^{|\bar{S}|+1}$ possible inputs they received by encoding it in a $d^{|\bar{S}|}$-dimensional quantum system. From the above result, the average success probability of B correctly guessing the inputs of R—and therefore winning the game—cannot be better than $1/d$, which is indeed the desired result.

Appendix B: Proof of Result 2

Here we present the proof of Eq. (10). We begin with a useful lemma, which is straightforward:

Lemma 3. *Let σ_{AB} be a bipartite density matrix in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $0 \leq M \leq \mathbb{1}$ (resp. N) be a symmetric operator on $\mathcal{H}_A$ (resp. $\mathcal{H}_B$). Let $\sigma_A = \text{tr}_B[\sigma_{AB}]$. Then the following inequality holds:*

$$\text{tr}_{AB}[\sigma_{AB}(M \otimes N)] \leq \text{tr}_A[\sigma_A M]\, \lambda_{\max}[N]. \tag{B1}$$

Proof. Let $N = \sum_i n_i |i\rangle\langle i|$ be the spectral decomposition of N. Remark that $\sigma_A^{(i)} = \langle i|\sigma_{AB}|i\rangle$ is an (unnormalised) positive semidefinite operator. We then have $\text{tr}_{AB}[\sigma_{AB}(M \otimes N)] = \sum_i n_i \,\text{tr}_A\left[\sigma_A^{(i)} M\right] \leq \lambda_{\max}[N]\,\text{tr}_A\left[\sum_i \sigma_A^{(i)} M\right] = \lambda_{\max}[N]\,\text{tr}_A[\sigma_A M]$. □

Equipped with this lemma, we can now prove the statement of Eq. (10). Party B performs a measurement with d^n different possible outcomes, described by measurement operators $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ with $M_{\mathbf{b}} \geq 0$ and $\sum_{\mathbf{b}} M_{\mathbf{b}} = \mathbb{1}$. Let SEP be the set of strings $\mathbf{b}$ for which $M_{\mathbf{b}}$ is a separable measurement operator, with $|\text{SEP}| \geq k$; for $\mathbf{b} \in \text{SEP}$ we thus have $M_{\mathbf{b}} = \sum_i \bigotimes_{k=1}^n M_{\mathbf{b},i}^{(k)}$. We will initially assume for simplicity that these separable POVM elements have the simpler tensor product form $M_{\mathbf{b}} = \bigotimes_{k=1}^n M_{\mathbf{b}}^{(k)}$; we will see later that, because of the linearity of $\mathcal{A}_{n,d}$, the proof nonetheless holds for arbitrary separable operators.

The parties $A_1, \ldots, A_n$ may perform arbitrary transformations $\mathcal{T}_{x_k y_k}^{(k)}$, which are formally represented by completely positive trace-preserving (CPTP) maps. Such transformations can always be written as a unitary $U_{x_k y_k}^{(k)}$ applied jointly to the local system and some environment state $\xi_{\mathcal{E}_k}$, with the environment being subsequently traced out. Formally, we have

$$\mathcal{T}_{x_k y_k}^{(k)} : \sigma \mapsto \text{tr}_{\mathcal{E}_k}\left[U_{x_k y_k}^{(k)}(\sigma \otimes \xi_{\mathcal{E}_k}) U_{x_k y_k}^{(k)\dagger}\right]. \tag{B2}$$

We denote the Hilbert space for each party by $\mathcal{S}_k$ and the total Hilbert space of the parties by $\mathcal{S} = \bigotimes_{k=1}^n \mathcal{S}_k$. Similarly, we denote the local and total Hilbert spaces of the environment by $\mathcal{E}_k$ and $\mathcal{E} = \bigotimes_{k=1}^n \mathcal{E}_k$, respectively. The total initial environment state is thus $\xi_{\mathcal{E}} = \bigotimes_{k=1}^n \xi_{\mathcal{E}_k}$. (Note that in our SDI scheme we only assume a bound on the dimension of the output space of each party so, *a priori*, this may be different from that of the input spaces so that the $U_{x_k y_k}^{(k)}$ instead map $\mathcal{S}_k^i \otimes \mathcal{E}_k^i \to \mathcal{S}_k^f \otimes \mathcal{E}_k^f$. For simplicity we assume the input and output spaces have the same dimensions in the proof below; the argument generalises trivially to the more general case.)

Evaluating explicitly $\mathcal{A}_{n,d}$, we have

$$\begin{aligned}
\mathcal{A}_{n,d} &= \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}} \left[\left(\bigotimes_{k=1}^{n} \mathcal{T}^{(k)}_{x_k y_k} \right) [\rho] \cdot M_{\mathbf{b}} \right] \\
&= \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}\mathcal{E}} \left[\left(\bigotimes_{k=1}^{n} U^{(k)}_{x_k y_k} \right) (\rho \otimes \xi_{\mathcal{E}}) \left(\bigotimes_{k=1}^{n} U^{(k)\dagger}_{x_k y_k} \right) (M_{\mathbf{b}} \otimes \mathbb{1}_{\mathcal{E}_k}) \right] \\
&= \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}\in\mathrm{SEP}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}\mathcal{E}} \left[(\rho \otimes \xi_{\mathcal{E}}) \bigotimes_{k=1}^{n} \left(U^{(k)\dagger}_{x_k y_k} \left(M^{(k)}_{\mathbf{b}} \otimes \mathbb{1}_{\mathcal{E}_k} \right) U^{(k)}_{x_k y_k} \right) \right] \\
&\qquad + \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}\notin\mathrm{SEP}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}\mathcal{E}} \left[(\rho \otimes \xi_{\mathcal{E}}) \left(\bigotimes_{k=1}^{n} U^{(k)\dagger}_{x_k y_k} \right) (M_{\mathbf{b}} \otimes \mathbb{1}_{\mathcal{E}_k}) \left(\bigotimes_{k=1}^{n} U^{(k)}_{x_k y_k} \right) \right] .
\end{aligned} \tag{B3}$$

Restricting ourselves to the first term above, we have

$$\begin{aligned}
T &\equiv \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}\in\mathrm{SEP}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}\mathcal{E}} \left[(\rho \otimes \xi_{\mathcal{E}}) \bigotimes_{k=1}^{n} \left(U^{(k)\dagger}_{x_k y_k} \left(M^{(k)}_{\mathbf{b}} \otimes \mathbb{1}_{\mathcal{E}_k} \right) U^{(k)}_{x_k y_k} \right) \right] \\
&\leq \frac{1}{d^{2n}} \sum_{\substack{\mathbf{x},\mathbf{y},\mathbf{b}\in\mathrm{SEP}:\\ \mathbf{b}=C(\mathbf{x},\mathbf{y})}} \mathrm{tr}_{\mathcal{S}_1\mathcal{E}_1} \left[(\rho_{\mathcal{S}_1} \otimes \xi_{\mathcal{E}_1}) \left(U^{(1)\dagger}_{x_1 y_1} \left(M^{(1)}_{b} \otimes \mathbb{1}_{\mathcal{E}_1} \right) U^{(1)}_{x_1 y_1} \right) \right] \prod_{k=2}^{n} \lambda_{\max}[M^{(k)}_{\mathbf{b}}],
\end{aligned} \tag{B4}$$

where $\rho_{\mathcal{S}_1} = \mathrm{tr}_{\mathcal{S}_2 \ldots \mathcal{S}_n} [\rho_{\mathcal{S}}]$ and we have used Lemma 3 $n-1$ times, together with the identity $\lambda_{\max}[U^{(k)\dagger}_{x_k y_k} (M^{(k)}_{\mathbf{b}} \otimes \mathbb{1}_{\mathcal{E}_k}) U^{(k)}_{x_k y_k}] = \lambda_{\max}[M^{(k)}_{\mathbf{b}}]$.

Since $\{M_{\mathbf{b}}\}_{\mathbf{b}}$ is a valid POVM it must satisfy $\sum_{\mathbf{b}} M_{\mathbf{b}} = \sum_{\mathbf{b}\in\mathrm{SEP}} \bigotimes_{k=1}^{n} M^{(k)}_{\mathbf{b}} + \sum_{\mathbf{b}\notin\mathrm{SEP}} M_{\mathbf{b}} = \mathbb{1}_{\mathcal{S}}$. Tracing out subsystems $\{2, \ldots, n\}$, we see that

$$\sum_{\mathbf{b}\in\mathrm{SEP}} M^{(1)}_{\mathbf{b}} \prod_{k=2}^{n} \mathrm{tr} \left[M^{(k)}_{\mathbf{b}} \right] = d^{n-1} \mathbb{1}_{\mathcal{S}_1} - \sum_{\mathbf{b}\notin\mathrm{SEP}} \mathrm{tr}_{\mathcal{S}_2 \cdots \mathcal{S}_n} [M_{\mathbf{b}}] . \tag{B5}$$

By noting that, given the values of $y_1, x_1, \ldots, x_{n-1}, \mathbf{b}$, the condition $\mathbf{b} = C(\mathbf{x}, \mathbf{y})$ fixes the values of the remaining variables and that these remaining variables do not appear in the summand in Eq. (B4), we can rewrite the summation simply over $y_1, x_1, \ldots, x_{n-1}, \mathbf{b}$. Noting also that $0 \leq \lambda_{\max}[P] \leq \mathrm{tr}\,[P]$ for any positive semidefinite operator P and using Eq. (B5) we have

$$\begin{aligned}
T &\leq \frac{1}{d^{2n}} \sum_{\substack{y_1, x_1, \ldots, x_{n-1},\\ \mathbf{b}\in\mathrm{SEP}}} \mathrm{tr}_{\mathcal{S}_1\mathcal{E}_1} \left[(\rho_{\mathcal{S}_1} \otimes \xi_{\mathcal{E}_1}) \left(U^{(1)\dagger}_{x_1 y_1} \left(M^{(1)}_{\mathbf{b}} \prod_{k=2}^{n} \lambda_{\max}[M^{(k)}_{\mathbf{b}}] \otimes \mathbb{1}_{\mathcal{E}_1} \right) U^{(1)}_{x_1 y_1} \right) \right] \\
&\leq \frac{1}{d^{2n}} \sum_{y_1, x_1, \ldots, x_{n-1}} \mathrm{tr}_{\mathcal{S}_1\mathcal{E}_1} \left[(\rho_{\mathcal{S}_1} \otimes \xi_{\mathcal{E}_1}) \left(U^{(1)\dagger}_{x_1 y_1} \left(\sum_{\mathbf{b}\in\mathrm{SEP}} M^{(1)}_{\mathbf{b}} \prod_{k=2}^{n} \mathrm{tr} \left[M^{(k)}_{\mathbf{b}} \right] \otimes \mathbb{1}_{\mathcal{E}_1} \right) U^{(1)}_{x_1 y_1} \right) \right] \\
&= \frac{1}{d^{2n}} \sum_{y_1, x_1, \ldots, x_{n-1}} \mathrm{tr}_{\mathcal{S}_1\mathcal{E}_1} \left[(\rho_{\mathcal{S}_1} \otimes \xi_{\mathcal{E}_1}) \left(U^{(1)\dagger}_{x_1 y_1} \left(d^{n-1} \mathbb{1}_{\mathcal{S}_1\mathcal{E}_1} - \sum_{\mathbf{b}\notin\mathrm{SEP}} \mathrm{tr}_{\mathcal{S}_2 \cdots \mathcal{S}_n} [M_{\mathbf{b}}] \otimes \mathbb{1}_{\mathcal{E}_1} \right) U^{(1)}_{x_1 y_1} \right) \right] \\
&\leq \frac{1}{d} - \frac{1}{d^{2n}} \lambda_{\max} \left[\sum_{y_1, x_1, \ldots, x_{n-1}} U^{(1)\dagger}_{x_1 y_1} \left(\sum_{\mathbf{b}\notin\mathrm{SEP}} \mathrm{tr}_{\mathcal{S}_2 \cdots \mathcal{S}_n} [M_{\mathbf{b}}] \otimes \mathbb{1}_{\mathcal{E}_1} \right) U^{(1)}_{x_1 y_1} \right] .
\end{aligned} \tag{B6}$$

We note briefly that one also obtains (B6) if one considers general separable operators of the form $M_{\mathbf{b}} = \sum_i \bigotimes_{k=1}^{n} M^{(k)}_{\mathbf{b},i}$ (rather than simple tensor products). This follows readily from the linearity of both Eqs. (B4) and (B5), so that the sum over separable measurement operators can be eliminated in the same way as above.

Continuing with the proof, note that for a positive semidefinite operator P in a d-dimensional Hilbert space, $\lambda_{\max}[P] \geq \frac{1}{d}\operatorname{tr}[P]$. Hence, letting D be the dimension of $\mathcal{E}_1$, we have

$$\begin{aligned} T &\leq \frac{1}{d} - \frac{1}{Dd^{2n+1}} \operatorname{tr}_{\mathcal{S}_1\mathcal{E}_1}\left[\sum_{y_1,x_1,\ldots,x_{n-1}} U^{(1)\dagger}_{x_1y_1}\left(\sum_{\mathbf{b}\notin\mathrm{SEP}} \operatorname{tr}_{\mathcal{S}_2\cdots\mathcal{S}_n}[M_{\mathbf{b}}]\otimes \mathbb{1}_{\mathcal{E}_1}\right)U^{(1)}_{x_1y_1}\right] \\ &= \frac{1}{d} - \frac{1}{Dd^{n+1}}\sum_{\mathbf{b}\notin\mathrm{SEP}} \operatorname{tr}_{\mathcal{S}\mathcal{E}_1}[M_{\mathbf{b}}\otimes \mathbb{1}_{\mathcal{E}_1}] \\ &\leq \frac{1}{d} - \frac{1}{d^{n+1}}\sum_{\mathbf{b}\notin\mathrm{SEP}} \lambda_{\max}[M_{\mathbf{b}}], \end{aligned} \tag{B7}$$

where, in the last step, we used the relation $\operatorname{tr}_{\mathcal{S}\mathcal{E}_1}[M_{\mathbf{b}}\otimes \mathbb{1}_{\mathcal{E}_A}] = D\operatorname{tr}_{\mathcal{S}}[M_{\mathbf{b}}] \geq D\lambda_{\max}[M_{\mathbf{b}}]$.

Substituting this back into the expression (B3) for $\mathcal{A}_{n,d}$ and noting that

$$\operatorname{tr}_{\mathcal{S}\mathcal{E}}\left[(\rho\otimes\xi_{\mathcal{E}})\left(\bigotimes_{k=1}^{n} U^{(k)\dagger}_{x_ky_k}\right)(M_{\mathbf{b}}\otimes \mathbb{1}_{\mathcal{E}_k})\left(\bigotimes_{k=1}^{n} U^{(k)}_{x_ky_k}\right)\right] \leq \lambda_{\max}[M_{\mathbf{b}}] \leq 1, \tag{B8}$$

we have the bound

$$\begin{aligned} \mathcal{A}_{n,d} &\leq \frac{1}{d} + \left(\frac{1}{d^n} - \frac{1}{d^{n+1}}\right)\sum_{\mathbf{b}\notin\mathrm{SEP}} \lambda_{\max}[M_{\mathbf{b}}] \\ &\leq \frac{1}{d} + \left(\frac{1}{d^n} - \frac{1}{d^{n+1}}\right)(d^n - k) \\ &= \frac{1}{d^n}\left(d^n - k + \frac{k}{d}\right), \end{aligned} \tag{B9}$$

as desired.

Appendix C: Partial tightness of Eq. (10) for two parties

In this section we consider the tightness of the inequality (10) for the bipartite case, which gives a lower bound on the number of entangled measurement operators compatible with a given average score $\mathcal{A}_{2,d}$. Specifically, we present a simple strategy that saturates the bound using a measurement for which there are $k = md$ separable measurement operators, for $m = 0,\ldots,d$.

Consider the following projective joint measurement of two d-dimensional quantum systems, in which the measurement operators $M_{\mathbf{b}} = |M_{\mathbf{b}}\rangle\langle M_{\mathbf{b}}|$ are separable for all (b_1,b_2) satisfying $b_2 - b_1 \in \{0,\ldots,m-1\}$, and entangled otherwise (where, as always, $b_2 - b_1$ is computed modulo d). Hence, there are md separable operators and $(d-m)d$ entangled operators. Specifically,

$$|M_{b_1b_2}\rangle = \begin{cases} |b_1,b_2\rangle & \text{for } b_2 - b_1 \in \{0,\ldots,m-1\}, \\ Z^{b_1}\otimes X^{b_2-b_1}|\phi_{\max}\rangle & \text{for } b_2 - b_1 \notin \{0,\ldots,m-1\}. \end{cases} \tag{C1}$$

To see that this is a valid measurement, note that all the inner products of two different separable basis-elements is zero. Similarly, the entangled basis-elements constitute a subset of the Bell-basis, and are thus orthonormal. To show that the inner products between the separable basis-elements and entangled basis-elements are all zero, consider the straightforward calculation

$$\langle b_1',b_2'|Z^{b_1}\otimes X^{b_2-b_1}|\phi_{\max}\rangle = \frac{1}{\sqrt{d}}\sum_{\ell=0}^{d-1}\omega^{\ell b_1}\langle b_1',b_2'|\ell,\ell+b_2-b_1\rangle = \frac{\omega^{b_1'b_1}}{\sqrt{d}}\delta_{b_2'-b_1',b_2-b_1}. \tag{C2}$$

Since all the separable basis-elements have $b_2' - b_1' \in \{0,\ldots,m-1\}$ while all entangled basis-elements have $b_2 - b_1 \notin \{0,\ldots,m-1\}$, the final delta function is zero. Hence, Eq. (C1) defines an orthonormal basis.

Consider thus the following strategy. Let A_1 and A_2 share a maximally entangled state, and apply (a relabelled variant of) the transformation strategy exploited several times in the main text, namely take the unitary transformations $U^{A_1}_{x_1y_1} = Z^{x_1}X^{y_1+x_1}$ and $U^{A_2}_{x_2y_2} = Z^{x_2}X^{y_2-x_2}$. It follows straightforwardly that

$$\mathcal{A}_{2,d} = \frac{d-m}{d} + \frac{m}{d^2}, \tag{C3}$$

which saturates the upper bound of Eq. (10) for any m. We leave it as an open question whether a similar partial tightness result holds in the more general n partite case.