Abstract for "Quantum Preparation Games"

Mirjam Weilenmann,[1,*] Edgar A. Aguilar,[1,†] and Miguel Navascués[1,‡]

[1] *Institute for Quantum Optics and Quantum Information (IQOQI) Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, AT*

(Dated: November 13, 2020)

Motivation. An important goal in information theory is to minimise the resources needed to perform various information processing tasks, for instance to find the most efficient ways to encode and transmit information over different types of channels or in the presence of adversaries. Resource theories are commonly used to quantify the resourcefulness of various building blocks. In quantum information processing, the resources are usually specific types of states, for instance entangled states, high-dimensional entangled states [1], or magic states [2].

To bring these theoretical insights to application, we need efficient and reliable schemes that certify resources of various types and this is what the framework of quantum preparation games provides. It is a theoretical basis for bridging the gap between theory and experiment. Namely, it allows us to derive optimal protocols to certify state resources of various resource theories. Our framework is highly adaptable, meaning that it can be employed to find the best protocols for resource certification in many different contexts, including the certification of particular quantum states or families of states, noisy state preparations or systems interacting with an environment that is itself in an unknown state. We can furthermore take restrictions on the possible measurements that can be used for detecting the quantum systems into account, which may for instance arise due to the choice of a particular experimental implementation. These restrictions can go as far as to only allow a particular finite set of few measurements.

We demonstrate the use of quantum preparation games on the example of entanglement detection. We are able to derive and analyse multi-round adaptive protocols in regimes that previous methods were unable to reach, allowing the optimisation of a moderate amount of round numbers (of the order of ~ 40). Unexpectedly, this work has led us to realise that adaptive protocols outperform non-adaptive ones in regimes where intuition and the current schemes employed in experiments indicate otherwise.

In the following we give a brief, non-technical account of the key results of our paper.

The framework of quantum preparation games. Assume a game where n quantum states from a source reach a referee one by one. On every received state, the referee can perform a measurement on the system and potentially adapt their measurement procedure depending on the round number $k \leq n$ and the previous history of measurement outcomes s_k. After n rounds the referee assigns a score to the source, who holds the role of the player in the preparation game.

In each round, the player prepares a state they send to the referee depending on k and on the previous history of outcomes obtained by the referee.[1] They are furthermore aware of the general measurement strategy the referee will follow (meaning the dependency of the referee's measurements on k and s_k) and of the scoring rule.

The expected score of a player with a preparation strategy $\mathcal{P}$ in a preparation game G is then

$$G(\mathcal{P}) \equiv \sum_s p(s|\mathcal{P}, G)\langle g(s)\rangle, \tag{1}$$

* mirjam.weilenmann@oeaw.ac.at

† edgar.aguilar@oeaw.ac.at

‡ miguel.navascues@oeaw.ac.at

[1] We can assume here, for simplicity, that the player holds no quantum memory. More details on when this assumption can be dropped are given in our technical article.

where $p(s|\mathcal{P}, G)$ denotes the probability that, conditioned on the player using a multi-round preparation strategy $\mathcal{P}$ in the game G, the final bit-string recorded by the referee is s.

A type of preparation game that is of particular interest are Maxwell-demon games. These are games where the referee's physical measurements in each round are taken from a finite set, which corresponds to the natural situation where an experimentalist performs a finite number of different measurements. In such a game we let the game configuration s_k in each round k include the whole history of previous measurement settings and outcomes.

Applications to entanglement detection. When aiming to certify entanglement, we consider a preparation game with a binary scoring rule with image $\{1, 0\}$, where 1 means that the certification succeeded, while 0 indicates failure. The usual type-I and type-II errors of the corresponding hypothesis test can be characterised in terms of the scores of different players in such a preparation game. In particular, when aiming to certify the entanglement of a particular state ρ the worst-case errors are $e_I = \max_{\mathcal{P}_{\text{sep}}} p(1|\mathcal{P}_{\text{sep}})$ and $e_{II} = p(0|\mathcal{P}_\rho)$ respectively, where $\mathcal{P}_{\text{sep}}$ are the strategies of a player restricted to produce separable states and $\mathcal{P}_\rho$ that of a player preparing ρ.

Applying these ideas to various types of multi-round protocols we reached the following two main insights. For further examples we refer to our article and for applications that certify high-dimensional entanglement to [3].

1) Advantages of adaptive strategies in Maxwell demon games.
Consider an n-round Maxwell demon game with a fixed set of possible measurements $\mathcal{M}(k)$ in round k. Now let us consider two scenarios. In scenario (A) the referee decides beforehand on a strategy for the measurement process, meaning, he decides which measurement to choose in each round (where these choices may be correlated). In scenario (B), the referee may not only correlate his choice of measurement between rounds, he may also make these choices on the fly, depending on previous measurement outcomes, i.e., use an adaptive strategy.

We find that for entanglement certification adaptive strategies (scenario (B)) outperform fixed ones (scenario(A)). This is intuitive if the aim is to certify entangled states from a source that are known to be chosen from a set of multiple different states. Then a natural strategy would be to first measure the states for a few rounds to reach a guess as to which of the states is being prepared and then use the remaining rounds to estimate the optimal entanglement witness for this state. However, if the state to be certified is known beforehand, the first step is seemingly unnecessary. Nevertheless, we find that optimal adaptive strategies still outperform optimal fixed ones. A simple example for this is the certification of the entanglement of 3 copies of the state $\frac{1}{\sqrt{2}}(|00\rangle + |1+\rangle)$, where $\mathcal{M}(k) = \{M_x, M_y, M_z\}$ for $k = 1, 2, 3$ and where M_x, M_y, M_z denote the POVMs associated with the Pauli observables. This completely contradicts our intuition and the standard procedures, which rely on repeating an optimal 1-shot protocol. An explanation of this phenomenon lies in the fact that the players either prepare three entangled or three separable states. In this sense, and no matter how a player preparing separable states adapts his preparation each round, there is some correlation in the overall prepared states, which can be exploited by the referee.

2) Construction of efficient protocols for entanglement detection in few experimental rounds.
In addition to optimisations over Maxwell demon games, our work also provides heuristics on how to devise efficient n round protocols for entanglement detection. Contrary to Maxwell demon games these need only a classical memory that grows polynomially in the round number. We propose two main procedures to systematically construct such protocols and have analysed examples using each of them with $\sim 20 - 40$ rounds.

The first method is inspired by gradient descent [4] and most easily illustrated with an example. Consider the states $|\psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with unknown θ. To certify and quantify their

entanglement we can construct a family of witnesses $W(\theta)$, of which the $|\psi_\theta\rangle$ with matching θ are eigenstates. We then perform an adaptive protocol that probabilistically chooses between measuring W and its gradient in each round. Depending on the outcome, we update either our estimate of θ or of the witness W. This procedure gives us a way to quantify the entanglement of the states $|\psi_\theta\rangle$ and to reliably distinguish them from any separable states (as long as θ is not too close to a multiple of π).

The second method relies on a see-saw type optimisation [5, 6] that subsequently circles through the different rounds of a protocol, optimising the POVMs round by round. This latter approach has the advantage of not relying on a specific structure or parametrisation of the resources of interest. We show in our technical article that such an optimisation leads to small errors in relatively few rounds and supplement our findings with a MATLAB implementation that can be easily adapted to other applications.

Outlook. The framework of preparation games allows us to prove the soundness of general certification protocols. The protocols that we propose for entanglement detection are, as far as we know, the first adaptive protocols proposed for this task. Due to the efficiency already achieved with these simple examples, we expect this type of protocol to be further explored and refined.

Our finding that adaptive protocols manage to outperform their non-adaptive counterparts, illustrates that our framework leads to unexpected insights for entanglement detection. Beyond the direct impact of these results, this also hints that an application of our framework to other resource theories may be of immediate interest, as other unexpected features of optimal certification protocols may be uncovered this way. With the current push towards building a quantum computer, a second application of our results that should be particularly emphasized is the certification of magic states.

For the future, we aim to explore an extension of preparation games where the referee is allowed to make the received states interact with a quantum system of a fixed dimension. This scenario perfectly models the computational power of a Noisy Intermediate-Scale Quantum (NISQ) device. In view of recent achievements in experimental quantum computing, this class of games is thus expected to become more and more popular in quantum information theory.

---

[1] B. M. Terhal and P. Horodecki, Physical Review A **61**, 040301 (2000).

[2] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[3] X.-M. Hu, W.-B. Xing, Y. Guo, M. Weilenmann, E. A. Aguilar, X. Gao, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, Z. Wang, and M. Navascués, "Optimized detection of unfaithful high-dimensional entanglement," (2020), arXiv:2011.02217.

[4] S. Boyd, L. Xiao, and A. Mutapcic, lecture notes of EE392o, Stanford University, Autumn Quarter (2004).

[5] R. F. Werner and M. M. Wolf, Quantum Inf. Comput. **1**, 1 (2001).

[6] K. Pál and T. Vértesi, Phys. Rev. A **82**, 022116 (2010).