Supplementary material: Robust and versatile self-testing

Tzyh Haur Yang,[1] Tamás Vértesi,[2] Jean-Daniel Bancal,[1] Valerio Scarani,[1,3] and Miguel Navascués[4]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science drive 2, Singapore 117543*
[2] *Institute for Nuclear Research, Hungarian Academy of Sciences, H-4001 Debrecen, P.O. Box 51, Hungary*
[3] *Department of Physics, National University of Singapore, 2 Science drive 3, Singapore 117542*
[4] *School of Physics, University of Bristol, Tyndall Avenue, Bristol BS8 1TL (U.K.)*

We give additional information on the self-testing of partially entangled two-qutrit states presented in the main text. In this case, the observed statistics come from bipartite nonlocality experiments characterized by two inputs and ternary outcomes per party. Note that previously no method could achieve selftesting in this important scenario. As a by-product, we prove a conjecture from 2002 about the specific form of the state giving maximal quantum violation of the CGLMP inequality.

I. THE SWAP METHOD FOR CGLMP

We present here a more detailed description of the SWAP method for the CGLMP scenario, which was only briefly discussed in the main document. In a forthcoming publication [1], we will prove that the idea of transferring quantum information from and to the black boxes can be carried even further and generalized to any Bell non-locality scenario with arbitrary number of measurement settings and outcomes.

Here we focus on the CGLMP inequality [2], which requires two measurement settings on each side, with three possible measurement outcomes. The inequality reads:

$$\begin{aligned} &\mathcal{B}_{\text{CGLMP}}(p) = \\ &p(a<b|x=1,y=1)+p(a>b|x=0,y=1) \\ +&p(a\geq b|x=1,y=0)+p(a<b|x=0,y=0) \;\geq 1. \end{aligned} \tag{1}$$

The maximum quantum violation of the above CGLMP inequality is conjectured [3] and verified numerically [4] to be $\mathcal{B}_{\text{CGLMP}}(p) = (12-\sqrt{33})/9 \approx 0.6950$. Moreover, it is believed that the maximal quantum violation can only be achieved with the (non-maximally entangled) state described in [2, 3]. Here we will also prove this conjecture true.

Firstly we give a strategy which is unitarily equivalent to the measurement scheme presented in references [2, 3] and achieves the maximal violation of CGLMP. The strategy is as follows: Alice's and Bob's first measurements $x, y = 0$ correspond to the projectors $\{|0\rangle\langle 0|, |1\rangle\langle 1|, |2\rangle\langle 2|\}$, namely $\overline{E}_a^0 = |a\rangle\langle a|$, $\overline{F}_b^0 = |b\rangle\langle b|$. The projectors corresponding to the other measurements $x, y, = 1$ are given by $\overline{E}_a^1 = |\omega_a\rangle\langle\omega_a|$, $\overline{F}_b^1 = |\omega_b\rangle\langle\omega_b|$, where $|\omega_i\rangle$ and the state to be measured $|\overline{\psi}\rangle$ are as follows

$$\begin{aligned} |\omega_k\rangle &= \frac{1}{3}\left(2|k\rangle + 2|k+1\rangle - |k+2\rangle\right), \\ |\overline{\psi}\rangle &= \frac{1}{3\sqrt{2+\gamma^2}}\Big((\gamma+\sqrt{3})(|00\rangle+|11\rangle+|22\rangle)+ \\ &\qquad \gamma(|01\rangle+|12\rangle+|20\rangle)+ \\ &\qquad (\gamma-\sqrt{3})(|02\rangle+|10\rangle+|21\rangle)\Big), \end{aligned} \tag{2}$$

where all addition above performed inside the kets are modulo 3 and $\gamma = (\sqrt{11}-\sqrt{3})/2$. This strategy up to local unitaries is equivalent to the measurement scheme presented in [2, 3], which involves complex coefficients.

The above measurements and states of Eq. (2) shall then be our reference system. Following the method presented in the main document, Alice and Bob will each attach a trusted qutrit initialized in state $|0\rangle$ to the entangled pair in order to certify the state. The next step is to construct the unitary operators which appear in the decomposition of the two-qutrit SWAP operator $S = TUVU$, with $U = \sum_{k=0}^2 P^k \otimes |k\rangle\langle k|$, $V = \sum_{k=0}^2 |k\rangle\langle k| \otimes P^{-k}$, $T = \mathbb{I} \otimes \sum_k |-k\rangle\langle k|$ and $P = \sum_{k=0}^2 |k+1\rangle\langle k|$. Clearly, we can take $\{E_k^0\}_{k=0}^2$, $\{F_k^0\}_{k=0}^2$ to play the role of the projectors $\{|k\rangle\langle k|\}_{k=0}^2$ in the first subsystem of the expressions above. A more challenging issue, though, is how to build the translation operator P from the measurement projectors defined in Eq. (2).

There are many choices to do so; we chose the simplest combination:

$$P = \sum_{i=0}^2 E_i^0\left(-\frac{1}{2}E_i^1 - 2E_{i+1}^1 + E_{i+2}^1\right) \tag{3}$$

which indeed is a translation operator mapping $|0\rangle \to |1\rangle \to |2\rangle \to |0\rangle$ whenever the measurement operators are $E_a^x = \overline{E}_a^x$. Since Alice and Bob's optimal operators are identical, the above formula also applies to Bob's settings if we replace E's by F's.

$P(E^x$

Note that the choice above in (4), contrary to the CHSH scenario [5], defines a valid unitary operator only for the optimal strategy of Ref. (2). However, in the device independent scenario, when the violation is not optimal, measurement operators can differ from (2) so that P is not unitary anymore. We address this problem by introducing an extra auxiliary operator, $\hat{P}_A$, which is unitary by construction, and satisfies the constraint that

how does it ensure the new S functions the same way?

$$\hat{P}_A^\dagger P(E_a^x) \geq 0. \tag{4}$$

We then use this operator $\hat{P}$ in the construction of the SWAP instead of P, thus ensuring that S is always unitary.

For Bob's side, the swap operators are defined exactly the same way as above for Alice. Thus, we require also another auxiliary operator $\hat{P}_B$. In the SDP, the conditions (5) for Alice and Bob are relaxed by requiring the positivity of two semidefinite, so-called localizing matrices $\Gamma(\hat{P}_A^\dagger P(E_a^x))$, $\Gamma(\hat{P}_B^\dagger P(F_b^y))$, where Γ refers to the moment matrix of [4] that proceeds from a quantum realization.

Putting all together, the estimation of the fidelity of the state inside the box $|\psi\rangle$ with respect to the reference state $|\overline{\psi}\rangle$ in Eq. (2) can be relaxed to the following SDP program:

$$\begin{aligned}
f = \min \quad & \langle\overline{\psi}|\rho_{\text{swap}}|\overline{\psi}\rangle \\
\text{such that} \quad & c \in \mathcal{Q}_n \\
& \sum_{a,b,x,y} B_{a,b}^{x,y} c_{E_a^x F_b^y} = \mathcal{B}_{\text{CGLMP}} \\
& \rho_{\text{swap}} \geq 0, \quad \text{Tr}(\rho_{\text{swap}}) = 1 \\
& \Gamma(\hat{P}_A^\dagger P(E_a^x)) \geq 0, \quad \Gamma(\hat{P}_B^\dagger P(F_b^y)) \geq 0, \quad (5)
\end{aligned}$$

where $\mathcal{Q}_n$ is a relaxation of the quantum set defined by the positivity of the moment matrix $\Gamma \geq 0$ in a certain level of the NPA hierarchy [4], and $B_{a,b}^{x,y}$ defines the Bell coefficients of the CGLMP inequality in Eq. (1).

Notice that here all three semidefinite matrices can be taken real, since, for any feasible point $\Gamma, \Gamma(\hat{P}_A^\dagger P(E_a^x)), \Gamma(\hat{P}_B^\dagger P(F_a^x))$ of the corresponding complex SDP, the real matrices $\Re\{\Gamma\}, \Re\{\Gamma(\hat{P}_A^\dagger P(E_a^x))\}, \Re\{\Gamma(\hat{P}_B^\dagger P(F_a^x))\}$ are also positive semidefinite, satisfy the appropriate linear constraints and return the same state fidelity. This is the case because both the figure of merit and the localizing matrices can be expressed as *real* linear combinations of the momenta c.

We ran the SDP for various values of $\mathcal{B}_{\text{CGLMP}}$ for the lowest possible level of the NPA hierarchy which defines all moments appearing in the objective function. The result is shown in Figure 3 of the main document. In particular, the fact that up to numerical precision $\langle\overline{\psi}|\,\rho_{\text{swap}}\,|\overline{\psi}\rangle = 1$ when the violation is maximal shows that any quantum system violating the CGLMP inequality maximally is indeed unitarily equivalent to $|\overline{\psi}\rangle$ proving the conjecture of Acin et al. [3] true.

$U^\dagger V^\dagger U^\dagger X^\dagger X U V U$

$P^{\dagger k} P^k \otimes |k\rangle\langle k|$

$P^\dagger \hat{P}_A \hat{P}_A^\dagger P$ 1

$P^\dagger P$

[1] Y. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani and M. Navascues, in preparation. *Note to the editors and referees: we are working to have this paper referenced in the arXiv by the time the present one is (hopefully) published in PRL.*

[2] D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).

[3] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, Phys. Rev. A 65, 052325 (2002).

[4] M. Navascués, S. Pironio and A. Acín, Phys. Rev. Lett. **98** 010401 (2007).

[5] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

$S = TUVU$;