A universal scheme for robust self-testing in the prepare-and-measure scenario arXiv:2003.01032

Nikolai Miklin[1] and Michał Oszmaniec[2]

[1] *ICTQT, University of Gdansk, Poland*
[2] *Center for Theoretical Physics, PAS, Warsaw, Poland*

Introduction.— With the increasing complexity of quantum systems, there is a growing need for certification and verification of their performance. This task is usually realized via the combination of quantum tomography and various benchmarking schemes, which, however, depend on the assumptions about the inner workings of quantum systems. In contrast to these approaches, *self-testing* [1] is a method which aims at proving the uniqueness of the implemented states or measurements based solely on the observed statistics and under minimal physical assumptions. The most know self-testing result is certification of the singlet state in the case of maximal violation of the CHSH Bell inequality [2]. More recently, a lot of interest has been directed at self-testing in the prepare-and-measure scenarios that is more experimentally appealing as compared to Bell's (see e.g. [3, 4]). Therein, one party, Alice, prepares a physical system in some state of her choice and sends it to Bob, who measures it. In order to get meaningful certification results in this work we assume that the dimension of the quantum system used for transmitting information is bounded from above.

Summary of the results.— In this work we propose an analytical method allowing to certify, in the SDI way, overlaps between preparations of arbitrary pure states and arbitrary projective measurements in *qudit* systems. The method is universally applicable and robust to experimental noise. This result allows for robust SDI certification of numerous properties such as MUB conditions [4], information-completeness of measurements [5], and SIC relations [6]. Moreover, for qubits our SDI certification leads to a full robust self-testing result.

Description of the scenario.— Let ϱ_a^x denote Alice's *target* preparation states with the choice of state specified by $x \in [n]$ and $a \in [d]$. Let Bob's *target* measurements be described by PVMs $(M_1^y, M_2^y, \dots, M_d^y)$, with $y \in [n]$ and $b \in [d]$. We assume that the parties do not have access to any entangled states or shared randomness (the relaxation of this assumption is possible arXiv:2003.01032). In this case the *target* statistics obey $p(b|a,x,y) = \mathrm{tr}(\varrho_a^x M_b^y)$. Let the corresponding *experimental* counterparts be denoted as $\tilde{\varrho}_a^x$ and $\tilde{M}_b^y$. In the SDI framework we assume that all states and measurements are defined on the same Hilbert space with dimension no greater than $d \in \mathbb{Z}_+$.

Result 1: Certification of overlaps.— Let us first consider the case of perfect statistics, i.e., $\tilde{p}(b|a,x,y) = p(b|a,x,y)$. Let us also assume that $p(b|a,x,y) = \delta_{a,b}$, whenever $y = x$, i.e., the states ϱ_a^x and effects M_a^x are "perfectly aligned". Due to the dimension assumption we can easily conclude that $\tilde{\varrho}_a^x = \tilde{M}_a^x$, for all $a \in [d]$ and $x \in [n]$. From here it follows that $\mathrm{tr}(\tilde{\varrho}_a^x \tilde{\varrho}_b^y) = \mathrm{tr}(\tilde{\varrho}_a^x \tilde{M}_b^y) = \tilde{p}(b|a,x,y) = \mathrm{tr}(\varrho_a^x \varrho_b^y)$, i.e., the overlaps between experimental states match the ones of the target states. The same holds for PVMs of Bob. Below we state our result on the robustness.

Theorem 1. *Let $|\tilde{p}(b|a,x,y) - p(b|a,x,y)| \leq \varepsilon, \forall a,b,x,y$. The proposed scheme is robust to noise in the sense that*

$$\sum_{a=1}^{d} \| \tilde{\varrho}_a^x \| \geq d(1-2\varepsilon) \quad \sum_{b=1}^{d} \left\| \tilde{M}_b^y \right\| \geq d(1-\varepsilon), \ \forall x, y,$$

and, for all $x \neq x'$, $a \neq a'$, $y \neq y'$, and $b \neq b'$:

$$|\mathrm{tr}(\tilde{\varrho}_a^x \tilde{\varrho}_{a'}^{x'}) - \mathrm{tr}(\varrho_a^x \varrho_{a'}^{x'})| \leq \varepsilon + \sqrt{2\varepsilon + d^2\varepsilon^2},$$
$$|\mathrm{tr}(\tilde{M}_b^y \tilde{M}_{b'}^{y'}) - \mathrm{tr}(M_b^y M_{b'}^{y'})| \leq \varepsilon + (1+d\varepsilon)\sqrt{2\varepsilon + d^2\varepsilon^2}\ .$$

Result 2: Self-testing of qubits.– For qubits certification of overlaps allows to prove robust self-testing result.

Theorem 2. *Let $d = 2$ and the conditions of Theorem 1 hold. Then there exist ε_0 such that for $\varepsilon \leq \varepsilon_0$ there exist $U \in \mathrm{SU}(2)$ (and possibly transposition $(\cdot)^{(T)}$) such that*

$$\frac{1}{2n}\sum_{a,x} \mathrm{tr}(U(\tilde{\varrho}_a^x)^{(T)} U^\dagger \varrho_a^x) \geq 1 - f(\varepsilon),$$
$$\frac{1}{2n}\sum_{b,y} \mathrm{tr}(U(\tilde{M}_b^y)^{(T)} U^\dagger M_b^y) \geq 1 - g(\varepsilon), \qquad (1)$$

where functions $f, g : [0, \varepsilon_0) \to \mathbb{R}_+$ depend solely on the target states and measurements and $f(\varepsilon) \propto \varepsilon$, $g(\varepsilon) \propto \varepsilon$ for small ε.

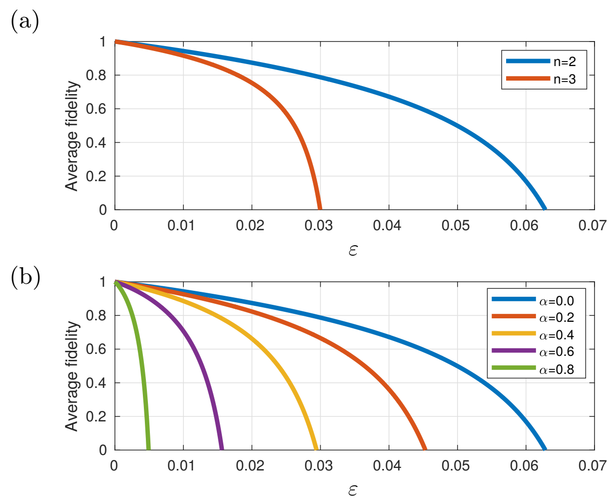

FIG. 1. Examples: (a) presents results for $n = 2, 3$ qubit MUBs. (b) presents results for two qubit bases for different degree of bias α. Value $\alpha = 0$ corresponds to two MUBs while $\alpha = 1$ gives two identical bases.

[1] D. Mayers and A. Yao, arXiv preprint quant-ph/0307205 (2003).
[2] S. Popescu and D. Rohrlich, Physics Letters A **169**, 411 (1992).
[3] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Physical Review A **98**, 062307 (2018).
[4] M. Farkas and J. Kaniewski, Physical Review A **99**, 032316 (2019).
[5] G. d'Ariano, P. Perinotti, and M. Sacchi, Journal of Optics B: Quantum and Semiclassical Optics **6**, S487 (2004).
[6] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Journal of Mathematical Physics **45**, 2171 (2004).