

Device-independent certification of tensor products of quantum states using single-copy self-testing protocols

Ivan Šupić¹, Daniel Cavalcanti², and Joseph Bowles²

¹Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland

²ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

05.03.2021.

Self-testing protocols are methods to determine the presence of shared entangled states in a device independent scenario, where no assumptions on the measurements involved in the protocol are made. A particular type of self-testing protocol, called parallel self-testing, can certify the presence of copies of a state, however such protocols typically suffer from the problem of requiring a number of measurements that increases with respect to the number of copies one aims to certify. Here we propose a procedure to transform single-copy self-testing protocols into a procedure that certifies the tensor product of an arbitrary number of (not necessarily equal) quantum states, without increasing the number of parties or measurement choices. Moreover, we prove that self-testing protocols that certify a state and rank-one measurements can always be parallelized to certify many copies of the state. Our results suggest a method to achieve device-independent unbounded randomness expansion with high-dimensional quantum states.

Introduction — Bell nonlocality describes measurement correlations which are rigidly incompatible with the notion of local determinism [Bel64, BCP⁺14]. Namely, all local deterministic theories satisfy bounds—called Bell inequalities—which limit the strength of the correlations between measurement outcomes of two spatially distant and non-communicating systems. Interestingly, it is possible to violate such Bell inequalities in quantum experiments [HBD⁺15, SMSC⁺15, GVW⁺15]. Such violating correlations, called nonlocal, are closely re-

lated to quantum resources such as entanglement and measurement incompatibility, essential for the development of modern day quantum technologies.

Bell nonlocality also plays a crucial role in so-called device-independent protocols. It turns out that the violation of a Bell inequality is a function of the observed correlations alone, regardless of the underlying physical realization. Thus, the sole observation of a Bell inequality violation witnesses the presence of both entanglement and incompatibility without having knowledge or making any assumptions about the underlying experimental implementation. Such an assumption-free verification is named *device-independent* and has a special significance in cryptographic scenarios [ABG⁺07, PAM⁺10].

The maximal violation of some Bell inequalities can even imply the precise form of the underlying state and measurements. This can be seen as a device-independent certification, and has received the name of self-testing [vB20, MY04]. The simplest example of such phenomenon is the maximal violation of the Clauser-Horn-Shimony-Holt (Bell) inequality [CHSH69], which can be used to self-test the maximally entangled pair of qubits and mutually unbiased local measurements [PR92, Tsi93, SW87].

There exist nonlocal correlations that self-test several copies of a quantum state, a process called parallel self-testing. These self-testing protocols have immediate applications in situations where high amounts of entanglement is needed, such as randomness expansion [CY14], parallel quantum key distribution [JMS20, Vid17], delegated quantum computing [RUV13, CGJV19], and universal entanglement certification [BŠCA18a]. One drawback of the first parallel self-testing proto-

cols is that they require a number of local measurements that increases exponentially with the number of copies one wants to certify [WBMS16, Col17, CN16, McK17, BŠCA18b]. This fact increases the time-cost and the randomness consumption of the protocol (relevant for cryptographic applications). More recently, techniques to reduce the number of local measurements to $\text{poly}(\log(n))$ and $\log(n)$ were found [NV17, NV18, CRSV18, OV16, BŠCA18b]. There exist protocols to self-test entangled states of arbitrary dimension with a constant number of three or four inputs per party [YN13, CGS17]. These protocols, when applied to copies of quantum states require making joint measurements between the local subsystems of each copy, making them challenging from an experimental perspective.

In this manuscript, we show a procedure to combine different self-testing protocols into a protocol that self tests tensor products of quantum states, without increasing the number of required measurements. The combined protocol has the advantage of not requiring joint measurements among the copies. As a key application, we show a way of self-testing n copies of the two-qubit maximally entangled state using only two measurements per party (see Figure 1 c). This is the first self-testing protocol using the minimum number of local measurements possible for certifying an unbounded amount of entanglement. This procedure can therefore be used to convert one random bit into an arbitrary number of private random bits.

Main idea of the method– For simplicity, we explain how our method can transform the Clauser-Horn-Shimony-Holt (CHSH) game into a self-test for n copies of a two-qubit maximally entangled state. The scenario consists of two space-like separated parties, Alice and Bob, making local measurements on a shared quantum system. Alice and Bob apply one of two measurements each, labeled $x = 0, 1$ and $y = 0, 1$ respectively, and their goal is to obtain outputs $a = 0, 1$ and $b = 0, 1$ such that $a \oplus b = x \cdot y$ where \oplus is addition modulo 2. Their score is defined as $\omega = \frac{1}{4} \sum_{x,y} P(a \oplus b = x \cdot y | x, y)$, *i.e.* the probability of satisfying the winning condition averaged over a uniform choice of x, y . Alice and Bob can use quantum resources to increase their score. In that case the inputs denote the measurement choices, while the out-

puts are simply measurement results. When they share quantum state ρ_{AB} , Alice performs measurements $\{M_{a|x}\}_{a,x}$, and Bob $\{N_{b|y}\}_{b,y}$ the probabilities $p(a, b|x, y)$ satisfy the Born rule $p(a, b|x, y) = \text{tr} [M_{a|x} \otimes N_{b|y} \rho_{AB}]$. The measurement observables are defined as $A_x = M_{0|x} - M_{1|x}$ and $B_y = N_{0|y} - N_{1|y}$. If Alice and Bob make use of classical resources (or separable states), the best score they can achieve is $\omega = \frac{3}{4}$, which is equivalent to satisfying the CHSH Bell inequality

$$\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2, \quad (1)$$

where $\langle A_x B_y \rangle = \sum_{ab} (-1)^{a+b} P(a, b|x, y)$. On the other hand, if they share a maximally entangled pair of qubits $|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$, Alice's measurements correspond to the Pauli observables $A_0 = \sigma_Z$ and $A_1 = \sigma_X$ and Bob's measurements to $B_0 = (\sigma_Z + \sigma_X)/\sqrt{2} \equiv \sigma_+$ and $B_1 = (\sigma_Z - \sigma_X)/\sqrt{2} \equiv \sigma_-$, they can achieve the score $\omega_q \approx 0.8536$. This strategy violates the CHSH Bell inequality to a value of $2\sqrt{2}$, and is the largest violation possible in quantum theory. This maximum value is also known to self-test the state $|\phi^+\rangle$. Thus, up to a possible local change of basis and extra unused degrees of freedom, the state $|\phi^+\rangle$ is the only state that achieves this value.

The CHSH inequality can also be used to self-test n copies of $|\phi^+\rangle^{\otimes n}$ via parallel self-testing [Col17, McK17]. For that purpose Alice and Bob in each round receive n -bit inputs $\mathbf{x} = (x_1, x_2, \dots, x_n)$ and $\mathbf{y} = (y_1, y_2, \dots, y_n)$, and return n -bit outputs $\mathbf{a} = (a_1, a_2, \dots, a_n)$ and $\mathbf{b} = (b_1, b_2, \dots, b_n)$. To self-test the state, Alice measures σ_Z or σ_X on her local qubit i depending on $x_i = 0, 1$, and Bob does similarly, measuring σ_+ or σ_- depending on $y_i = 0, 1$ and returning outcome b_i (see Fig. 1b). The resulting correlations maximally violate n CHSH inequalities in parallel and imply Alice and Bob share a tensor product of n maximally entangled pairs of qubits.

We consider, in turn, a scenario in which each party has only two choices of measurements $x = 0, 1$ and $y = 0, 1$ (Fig. 1c). If $x = 0$ Alice measures all of her qubits in the σ_Z -basis, whereas if $x = 1$ she measures all of them in the σ_X -basis. In both cases she returns an output consisting of n bits $\mathbf{a} = (a_1, a_2, \dots, a_n)$ corresponding to the outcomes of each of the n measurements. Bob proceeds similarly, measuring all

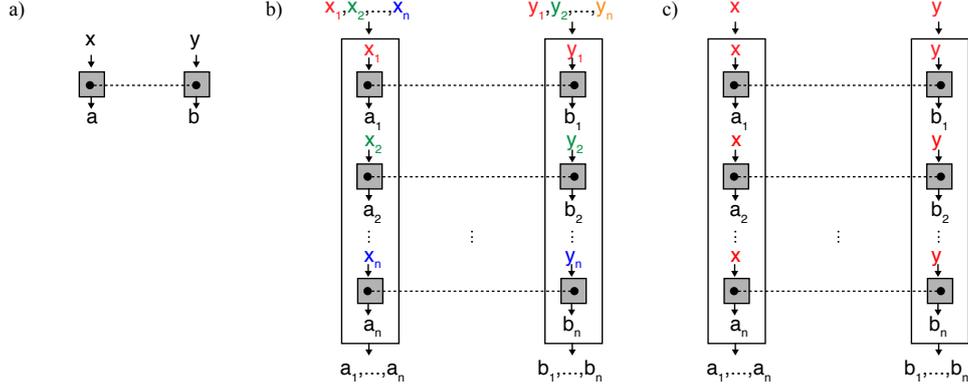


Figure 1: a) Standard Bell scenario, where local measurements labeled by x and y with outcomes a and b are performed on a shared state. b) Standard parallel self-testing protocol certifying n copies of a quantum states. The measurement choice corresponds to a string of n elements, each of them used to determine the measurement applied to each copy. Thus, the total number of local measurements increases exponentially with the number of copies one aims at certifying. c) The procedure we propose here (see Theorem 1) transforms a self-testing protocol for a single quantum state into a protocol for an arbitrary number of copies. Each party applies the same measurement to each copy and outputs each individual outcome.

his qubits in σ_+ and σ_- bases and returning $\mathbf{b} = (b_1, b_2, \dots, b_n)$. For any pair (a_i, b_i) , the condition $P(a_i \oplus b_i = x \cdot y) = \omega_q$ is satisfied, and one might naively think that this information alone is enough to conclude that the state is $|\phi^+\rangle^{\otimes n}$. This would be a mistake however, as the following counter-example shows. Suppose Alice and Bob measure a single copy of $|\phi^+\rangle$, obtaining outputs a, b such that $P(a \oplus b = x \cdot y) = \omega_q$. Then, they set $a_i = a$ and $b_i = b$ for all i , leading to $P(a_i \oplus b_i = x \cdot y) = \omega_q$ for all i . Thus, one can achieve $P(a_i \oplus b_i = x \cdot y) = \omega_q$ for all i with only a single copy of $|\phi^+\rangle$.

One thus needs to consider more information than just the CHSH score of each copy. One possibility is to consider the marginal statistics, since in the parallel n -copy strategy one has $p(\mathbf{a}|x) = 1/2^n$ whereas in the single-copy strategy the local output bits a_i are always perfectly correlated (with a similar situation for Bob). However this will not work, since by using n bits of pre-shared randomness $(\lambda_1, \dots, \lambda_n)$ and post-processing their outputs according to $a_i = a + \lambda_i$ and $b_i = b + \lambda_i$, the local output bits of the single-copy strategy can be decorrelated without affecting the CHSH scores. Notice however, that there is still a crucial difference between the two strategies that remains: in each round of the single-copy strategy, if the first pair satisfies $a_1 + b_1 = x \cdot y$, then all other pairs also satisfy $a_i + b_i = x \cdot y$. This is not the case for the n -copy strategy, where each pair has a probability ω_q to

satisfy the condition in each round, independent of the other pairs. It is precisely this difference that we use as an inspiration to design our self-testing protocol.

The main result— Before stating our main result, let us define self-testing in a precise way. Consider a general bipartite Bell scenario, where $x, y \in \{0, 1, \dots, m-1\}$ and $a, b \in \{0, 1, \dots, o-1\}$. Alice and Bob share the state $\rho_{AB} = \text{tr}_P[|\psi\rangle\langle\psi|_{ABP}]$, with $|\psi\rangle_{ABP}$ being any purification of ρ_{AB} .

The probabilities of obtaining outputs a and b , when the inputs are x and y , respectively, are given by

$$p(a, b|x, y) = \langle\psi|M_{a|x} \otimes N_{b|y} \otimes \mathbb{1}_P|\psi\rangle, \quad (2)$$

where $\{M_{a|x}\}$ and $\{N_{b|y}\}$ are Alice's and Bob's local measurement operators. We say that the probabilities $\{p(a, b|x, y)\}$ self-test the reference experiment $\{|\psi'\rangle_{A'B'}, M'_{a|x}, N'_{b|y}\}$ if observing them in an experiment implies the existence of a local unitary transformation $U = U_{AA'} \otimes V_{BB'} \otimes \mathbb{1}_P$ such that

$$\begin{aligned} U[|\psi\rangle_{ABP} \otimes |00\rangle_{A'B'}] &= |\xi\rangle_{ABP} \otimes |\psi'\rangle_{A'B'}; \\ U[M_{a|x} \otimes N_{b|y} \otimes \mathbb{1}_P|\psi\rangle_{ABP} \otimes |00\rangle_{A'B'}] &= \\ &= |\xi\rangle_{ABP} \otimes (M'_{a|x} \otimes N'_{b|y}|\psi'\rangle_{A'B'}). \end{aligned} \quad (3)$$

These equations state that, up to ancillary degrees of freedom and local basis transformations, the state $|\psi\rangle$ is equivalent to $|\psi'\rangle$, and the measurements $M_{a|x}$ and $N_{b|y}$ act on $|\psi\rangle$ in the same

way as $M'_{a|x}$ and $N'_{b|y}$ act on $|\psi'\rangle$. The state $|\xi\rangle$ is usually called the junk state and it can be seen as the state of additional degrees of freedom. Finally, let us define a Bell expression \mathcal{I} , as a linear combination of experimental probabilities $\mathcal{I} = \sum_{abxy} b_{a,b}^{x,y} p(a, b|x, y)$, where $b_{a,b}^{x,y} \in \mathbb{R}$.

Now we can state our main result:

Theorem 1. *Consider a Bell expression \mathcal{I} and $\{p(a, b|x, y)\}$ for a scenario where Alice and Bob have m inputs and o outputs each, such that the value $\mathcal{I}(\{p(a, b|x, y)\}) = \beta$ self-tests the reference experiment $R = \{|\psi'\rangle, M'_{a|x}, N'_{b|y}\}$, where $M'_{a|x}, N'_{b|y}$ are rank-one projectors and $p(a, b|x, y) > 0 \forall a, b$ for each combination (x, y) appearing in \mathcal{I} . Consider the scenario of Fig. 1b with m inputs and o^n outputs per party. Then, there exists a collection of n non-linear Bell expressions \mathcal{J}^i ($i = 1, \dots, n$) for this scenario that self-test the reference experiment $R_n = \{|\psi'\rangle^{\otimes n}, \otimes_{i=1}^n M'_{a_i|x}, \otimes_{i=1}^n N'_{b_i|y}\}$.*

The nonlinear Bell expressions \mathcal{J}^i in Theorem 1 are constructed as follows. Define $\mathcal{I}^1 = \mathcal{I}(\{p(a_1, b_1|x, y)\})$ and the conditional Bell expressions for the pair $i > 1$ as

$$\mathcal{I}_{\mathbf{a}_{i-1}\mathbf{b}_{i-1}}^i = \mathcal{I}(\{p(a_i, b_i|x, y, \mathbf{a}_{i-1}, \mathbf{b}_{i-1})\}), \quad (4)$$

where $\mathbf{a}_{i-1} = (a_1, a_2, \dots, a_{i-1})$ and $\mathbf{b}_{i-1} = (b_1, b_2, \dots, b_{i-1})$. $\mathcal{I}_{\mathbf{a}_{i-1}\mathbf{b}_{i-1}}^i$ gives the value of \mathcal{I} for the pair i conditioned on observing the particular values $\mathbf{a}_{i-1} = (a_1, a_2, \dots, a_{i-1})$ and $\mathbf{b}_{i-1} = (b_1, b_2, \dots, b_{i-1})$. Note that in order for these conditional Bell expressions to be well defined we require that $p(\mathbf{a}_{i-1}, \mathbf{b}_{i-1}|x, y) > 0 \forall \mathbf{a}_{i-1}, \mathbf{b}_{i-1}$ for each combination (x, y) appearing in \mathcal{I} . This is automatically the case for the reference experiment R_n due to the properties of R given in the statement of the theorem. The Bell expression \mathcal{J}^i is defined as

$$\mathcal{J}^i = \frac{1}{o^{2(i-1)}} \sum_{\mathbf{a}_{i-1}\mathbf{b}_{i-1}} \mathcal{I}_{\mathbf{a}_{i-1}\mathbf{b}_{i-1}}^i, \quad (5)$$

for $i > 1$ and $\mathcal{J}^1 = \mathcal{I}^1$. The observation that $\mathcal{J}^i = \beta \forall i = 1, \dots, n$ self tests R_n . The proof is inductive (given a self-test of k copies, the value of \mathcal{J}^{k+1} self-tests an additional copy) and is given in the Appendix A. Here we provide some intuition behind the proof. As shown on the example of the CHSH inequality two ingredients are necessary to make a self-testing statement

with the minimal number of inputs. First, all sets of probabilities $p(a_i, b_i|x, y)$ reach the maximum of \mathcal{I} , and the pairs of outputs (a_i, b_i) are mutually independent. If \mathcal{J}^i takes value β for all i , it means that all conditional Bell expressions $\mathcal{I}_{\mathbf{a}_{i-1}\mathbf{b}_{i-1}}^i$ are also equal to β . It can be shown that the maximal values of conditional Bell expressions imply that the outputs corresponding to different i -s are mutually independent. In other words, conditioning on $\mathbf{a}_{i-1}, \mathbf{b}_{i-1}$ does not affect the values of a_i and b_i . Hence, $\beta = \mathcal{I}(p(a_i, b_i|x, y, \mathbf{a}_{i-1}, \mathbf{b}_{i-1})) = \mathcal{I}(p(a_i, b_i|x, y))$, for all i -s, which means that both conditions for making a self-testing statement are met.

A direct consequence of Theorem 1 is the possibility of self-testing n copies of the two-qubit maximally entangled state $|\phi^+\rangle$ (itself a maximally entangled state of local dimension 2^n) with only two measurement settings per party via the CHSH Bell inequality. More precisely, we have the following corollary:

Corollary 1. *Let $M_{a|x}, N_{b|y}$ ($x, y \in \{0, 1\}, a, b \in \{\pm 1\}$) be the local measurements that lead to the maximal violation of the CHSH Bell inequality when applied to $|\phi^+\rangle$. Then the correlations obtained by performing the experiment $R = \{|\phi^+\rangle, M_{a|x}, N_{b|y}\}$ in the parallel scheme of Fig. 1c self-test the reference experiment $\{|\phi^+\rangle^{\otimes n}, M_{a|x}^{\otimes n}, N_{b|y}^{\otimes n}\}$*

In particular, this means that an unbounded amount of entanglement can be certified in a device-independent manner with the minimum number of local measurements possible.

Although Theorem 1 holds only for the case of perfect statistics, one can investigate the robustness to noise of Corollary 1 for the case $n = 2$, via the technique proposed in [BNS⁺15, YVB⁺14]. The precise noise model we consider is one in which each copy of the state is subject to the same level of white noise. That is, the observed correlations are generated using the same measurement strategy on the state $\rho_\nu \otimes \rho_\nu$ where

$$\rho_\nu = \nu|\phi^+\rangle\langle\phi^+| + (1 - \nu)\mathbb{1}/4. \quad (6)$$

In [BNS⁺15, YVB⁺14] a semi-definite program is given that calculates a value f , such that for any state ρ_{AB} leading to the observed correlations, there exists a local transformation mapping ρ_{AB} to a state that has fidelity at least f with the reference state (in this case $|\phi^+\rangle \otimes |\phi^+\rangle$).

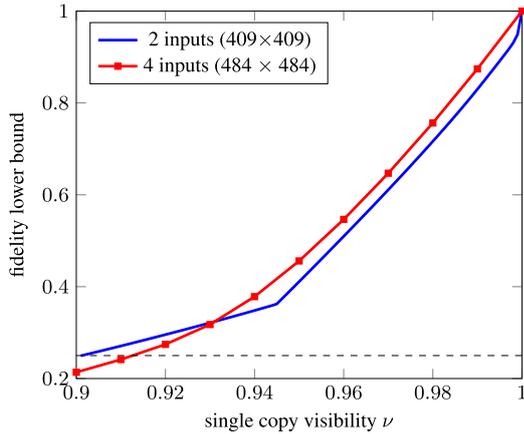


Figure 2: Lower bounds to the self-tested fidelity with the state $|\phi^+\rangle \otimes |\phi^+\rangle$ obtained via the method proposed in Refs. [BNS⁺15, YVB⁺14], using correlations obtained from two copies of the isotropic state $\nu|\phi^+\rangle\langle\phi^+| + (1-\nu)\mathbb{1}/4$. The blue curve is obtained using two inputs per party, using the parallel scheme of Fig. 1c. The red curve is data taken from [WBMS16] using the strategy of Fig. 1b with four inputs per party. The legend gives the size of the matrices used in the corresponding SDP optimization. The dashed line corresponds to the trivial fidelity between the target state and the separable state $|00\rangle$ of 0.25.

In the case of perfect self-testing (3), one has $f = 1$, which then decreases as a function of the noise parameter. Fig. 2 shows the values of f obtained as a function of ν for this noise model.

Extensions – Theorem 1 is defined for bipartite Bell inequalities that feature an equal number of inputs per party. Here we present some more general extensions to this result that either do not require the knowledge of a specific Bell inequality, or allow one to self-test tensor products of different bipartite states.

Parallel self-testing protocols from full statistics—While Theorem 1 refers to self-tests based on the maximal violation of some Bell inequality, it is worth noting that similar claims can be made for self-testing protocols based on the observation of a particular set of correlations. More precisely, we have the following result.

Theorem 2. *Assume that the correlations $\{p(a, b|x, y)\}$ self-test the reference state $|\psi'\rangle$, such that $p(a, b|x, y) > 0$ for all a, b, x, y . Then the correlations $\{p(\mathbf{a}, \mathbf{b}|x, y)\}$ obtained by performing the reference experiment n times in the parallel scheme of Fig. 1c self-test the corresponding tensor product $|\psi'\rangle^{\otimes n}$.*

In Appendix B we give an example of this technique that self-tests tensor products of the maximally entangled two-qubit state based on the correlations presented in [WWS16].

Combining self-testing protocols—The previous results show how it is possible to self-test a tensor product $|\psi'\rangle^{\otimes n}$ of the same state $|\psi'\rangle$, starting from a given protocol to self-test the state $|\psi'\rangle$. In fact, the following describes how our construction can also be used to generate self-testing protocols for a tensor product of different states $\otimes_i |\psi'_i\rangle$.

Theorem 3. *Consider a set of states $\{|\psi'_i\rangle\}$, each of which is self-tested through the maximal value of a corresponding Bell expression \mathcal{I}_i , where each \mathcal{I}_i features the same number of inputs for each party. Then the correlations $\{p(\mathbf{a}, \mathbf{b}|x, y)\}$ obtained by performing the reference experiments n times in the parallel scheme of Fig. 1c self-test the state $\otimes_i |\psi'_i\rangle$.*

The proof of this is almost identical to the proof of Theorem 1, instead now in (4) the Bell expressions \mathcal{I}_i are different for each i ; see Appendix C for more details. One implication of this is the possibility to self-test a tensor product of different partially entangled pairs of qubits with two inputs for each party, which can be achieved through the use of different tilted CHSH inequalities [BP15].

All self-testing protocols can be parallelized—Here we discuss conditions for parallel self-testing without aiming to keep the number of inputs constant. As mentioned in the introduction, a number of schemes to parallel self-test certain classes of states are known (see [Col17, McK17, CN16, KM18, BKM19]), where the number of inputs scales exponentially with the number of copies to be self-tested. Given these examples, one interesting question is thus whether any self-testing protocol for a state $|\psi\rangle$ can be ‘parallelized’ to self-test the tensor product $|\psi\rangle^{\otimes n}$, at the expense of having exponentially many inputs. We give a positive answer to this question, answering an even a more general question of self-testing a tensor product $\otimes_i |\psi_i\rangle$ of different states, given that there are self-tests for the individual states $|\psi_i\rangle$. Note that unlike the previous results, no restrictions are needed on the reference correlations (i.e. some probabilities can be zero).

Theorem 4. Consider a set of n bipartite Bell expressions $\{\mathcal{I}_i\}$ characterised by m_i inputs and o_i outputs, respectively, such that the value $\mathcal{I}_i(\{p(a_i, b_i | x_i, y_i)\}) = \beta_i$ self-tests the reference experiment $R_i = \{|\psi'_i\rangle, M'_{a_i|x_i}, N'_{b_i|y_i}\}$, where $M'_{a_i|x_i}, N'_{b_i|y_i}$ are rank-one projectors for each i . Then, the correlations obtained by performing the R_i 's in parallel as in Fig. 1b self-test the reference experiment $R_n = \{\otimes_{i=1} |\psi'_i\rangle, \otimes_i M'_{a_i|x_i}, \otimes_{i=1}^n N'_{b_i|y_i}\}$.

The result is proven by constructing a single Bell expression whose maximal value self-tests R_n . For each pair i define the Bell value conditioned on particular choice of other inputs $x_j, y_j, j \neq i$:

$$\mathcal{I}_{\mathbf{x}^{(i)}\mathbf{y}^{(i)}}^i = \sum_{\mathbf{a}^{(i)}, \mathbf{b}^{(i)}} \mathcal{I}_i(p(\mathbf{a}, \mathbf{b} | \mathbf{x}, \mathbf{y})) \quad (7)$$

where $\mathbf{a}^{(i)} = \{a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n\}$ and similarly for $\mathbf{b}^{(i)}, \mathbf{x}^{(i)}$ and $\mathbf{y}^{(i)}$. The Bell expression \mathcal{I}_i averaged over all other inputs $\mathbf{x}^{(i)}$ and $\mathbf{y}^{(i)}$ is

$$\mathcal{J}^i = \frac{1}{\prod_{j \neq i} m_j^2} \sum_{\mathbf{x}^{(i)}\mathbf{y}^{(i)}} \mathcal{I}_{\mathbf{x}^{(i)}\mathbf{y}^{(i)}}^i. \quad (8)$$

If \mathcal{J}^i achieves its maximal value, it means that for for every \mathbf{x}_i and \mathbf{y}_i $\mathcal{I}_{\mathbf{x}_i\mathbf{y}_i}^i$ also achieves the maximal value, which is enough to prove self-testing of the reference experiment R_n . The proof of the theorem is given in Appendix D.

Application: unbounded randomness expansion.— Self-testing is intrinsically related to device-independent randomness expansion [CY14, CK11, LLR⁺21]. This is because, once we certify that the system is in the state $|\psi\rangle$, we can also conclude that any external system is uncorrelated to it. Thus, an external observer can not predict the outcomes of the measurements applied to the system of interest, *i.e.* the outcomes are random. In particular, if the state is maximally entangled of local dimension d , and the measurements applied to it are rank-one projective, the amount of random bits obtained per round is $\log_2(d)$. Notice, however, that in a Bell test some initial amount of randomness must be consumed in the choice of inputs. Thus,

the efficiency of the randomness generation protocol is typically given by the trade-off between the initial randomness consumed and the final randomness obtained. Our Theorem 1 applied to the CHSH inequality and self-testing n copies of a maximally entangled state shows that the best trade-off can be achieved from the noiseless correlations, where only one bit of randomness is used to generate $\log_2(d)$ bits or randomness per round. We thus suspect that our results could improve extraction rates of practical device-independent randomness expansion protocols, although this would require a closer look at issues of noise robustness.

Discussion—In this manuscript we introduced a new procedure useful in parallel self-testing. It allows to self-test highly entangled quantum states with a constant number of measurements. Such schemes are important in protocols for randomness expansion: a small amount of randomness can be expanded to a string of unbounded length. At the heart of our construction lies an interesting insight: independent Bell violations can be used to ensure independence of sources even when the measurements are perfectly correlated. There are several directions for future research on the topic. It would be interesting to explore noise robustness of our scheme. Furthermore, the condition for self-testing can be seen as the maximal violation of a non-linear Bell inequality. One might try to understand if this can be achieved using a single linear Bell inequality.

Note— While working on this project we became aware of the work [SSKA19] exploring self-testing of quantum systems of arbitrary local dimension with minimal number of measurements.

Acknowledgements— We thank Jean-Daniel Bancal for sharing numerical data, to Jed Kaniewski and Yeong-Cherng Liang for useful comments and suggestions and to the anonymous referee for many useful comments. We acknowledge funding from SNSF (grant DIAQ), Ramon y Cajal fellowship, the Government of Spain (FIS2020-TRANQI, Retos Quspín and Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA, AGAUR SGR 1381), ERC AdG CERQUTE and the AXA Chair in Quantum Information Science.

References

- [ABG⁺07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007. doi:10.1103/PhysRevLett.98.230501.
- [BCP⁺14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014. doi:10.1103/RevModPhys.86.419.
- [Bel64] John Stewart Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964. URL: <https://cds.cern.ch/record/111654>.
- [BKM19] Spencer Breiner, Amir Kalev, and Carl A. Miller. Parallel self-testing of the GHZ state with a proof by diagrams. In Peter Selinger and Giulio Chiribella, editors, Proceedings of the 15th International Conference on *Quantum Physics and Logic*, Halifax, Canada, 3-7th June 2018, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 43–66. Open Publishing Association, 2019. doi:10.4204/EPTCS.287.3.
- [BNS⁺15] Jean-Daniel Bancal, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang. Physical characterization of quantum devices from nonlocal correlations. *Phys. Rev. A*, 91:022115, Feb 2015. doi:10.1103/PhysRevA.91.022115.
- [BP15] Cédric Bamps and Stefano Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Phys. Rev. A*, 91:052111, May 2015. doi:10.1103/PhysRevA.91.052111.
- [BŠCA18a] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, Oct 2018. doi:10.1103/PhysRevLett.121.180503.
- [BŠCA18b] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Self-testing of Pauli observables for device-independent entanglement certification. *Phys. Rev. A*, 98:042336, Oct 2018. doi:10.1103/PhysRevA.98.042336.
- [CGJV19] Andrea Coladangelo, Alex B Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 247–277. Springer, 2019. doi:10.1007/978-3-030-17659-4_9.
- [CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8:15485, may 2017. doi:10.1038/ncomms15485.
- [CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. doi:10.1103/PhysRevLett.23.880.
- [CK11] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011. doi:10.1088/1751-8113/44/9/095305.
- [CN16] Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid, 2016. arXiv:1609.06306. URL: <https://arxiv.org/abs/1609.06306>.
- [Col17] Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information and Computation*, 17(9-10):831–865, 2017. doi:10.26421/QIC17.9-10-6.
- [CRSV18] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, September 2018. doi:10.22331/q-2018-09-03-92.

- [CY14] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, pages 427–436, New York, NY, USA, 2014. ACM. doi:10.1145/2591796.2591873.
- [GVW⁺15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell’s theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015. doi:10.1103/PhysRevLett.115.250401.
- [HBD⁺15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, and et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015. doi:10.1038/nature15759.
- [JMS20] Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel device-independent quantum key distribution. *IEEE Transactions on Information Theory*, 66(9):5567–5584, Sep 2020. doi:10.1109/tit.2020.2986740.
- [KM18] Amir Kalev and Carl A Miller. Rigidity of the magic pentagram game. *Quantum Science and Technology*, 3(1):015002, 2018. doi:10.1088/1367-2630/18/2/025021.
- [LLR⁺21] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J Brown, Jun Zhang, Roger Colbeck, Jingyun Fan, et al. Device-independent randomness expansion against quantum side information. *Nature Physics*, pages 1–4, 2021. doi:10.1038/s41567-020-01147-2.
- [McK17] Matthew McKague. Self-testing in parallel with CHSH. *Quantum*, 1:1, April 2017. doi:10.22331/q-2017-04-25-1.
- [MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4:273, 2004. doi:10.26421/QIC4.4-3.
- [NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007. doi:10.1103/PhysRevLett.98.010401.
- [NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. doi:10.1088/1367-2630/10/7/073013.
- [NV17] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 1003–1015, New York, NY, USA, 2017. ACM. doi:10.1145/3055399.3055468.
- [NV18] Anand Natarajan and Thomas Vidick. Low-degree testing for quantum states, and a quantum entangled games pcp for qma. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 731–742, Oct 2018. doi:10.1109/FOCS.2018.00075.
- [OV16] Dimiter Ostrev and Thomas Vidick. The structure of nearly-optimal quantum strategies for the CHSH (n) XOR games. *Quantum Information & Computation*, 16(13-14), pp.(13-14):1191–1211, 2016. doi:10.26421/QIC16.13-14-6.
- [PAM⁺10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matuskevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by Bell’s theorem. *Nature*, 464(7291):1021–1024, 2010. doi:10.1038/nature09008.

- [PR92] Sandu Popescu and Daniel Rohrlich. Which states violate Bell’s inequality maximally? *Physics Letters A*, 169(6):411–414, 1992. doi:10.1016/0375-9601(92)90819-8.
- [RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456, 2013. doi:10.1038/nature12035.
- [SMSC⁺15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015. doi:10.1103/PhysRevLett.115.250402.
- [SSKA19] Shubhayan Sarkar, Debashis Saha, Jędrzej Kaniewski, and Remigiusz Augusiak. Self-testing quantum systems of arbitrary local dimension with the minimal number of measurements, 2019. arXiv:1909.12722.
- [SW87] Stephen J. Summers and Reinhard F. Werner. Maximal violation of Bell’s inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987. doi:10.1007/BF01207366.
- [Tsi93] Boris Tsirelson. Some results and problems on quantum Bell-type inequalities. *Hadronis Journal Supplement*, 8:329–45, 1993. URL: <https://ci.nii.ac.jp/naid/10026857475/en/>.
- [vB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, Sep 2020. doi:10.22331/q-2020-09-30-337.
- [Vid17] Thomas Vidick. Parallel DIQKD from parallel repetition, 2017. arXiv:1703.08508.
- [WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93:062121, 2016. doi:10.1103/PhysRevA.93.062121.
- [WWS16] Yukun Wang, Xingyao Wu, and Valerio Scarani. All the self-testings of the singlet for two binary measurements. *New Journal of Physics*, 18(2):025021, 2016. doi:10.1088/1367-2630/18/2/025021.
- [YN13] Tzyh Haur Yang and Miguel Navascués. Robust self-testing of unknown quantum systems into any entangled two-qubit states. *Phys. Rev. A*, 87:050102, May 2013. doi:10.1103/PhysRevA.87.050102.
- [YVB⁺14] Tzyh Haur Yang, Tamás Vértesi, Jean-Daniel Bancal, Valerio Scarani, and Miguel Navascués. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.*, 113:040401, Jul 2014. doi:10.1103/PhysRevLett.113.040401.

v

A Proof of Theorem 1

Before starting the proofs let us introduce some useful notation. The probabilities to observe outcomes $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ when the inputs are x and y are given by the Born rule:

$$p(\mathbf{a}, \mathbf{b}|x, y) = \text{tr}[M_{\mathbf{a}|x} \otimes N_{\mathbf{b}|y} \rho^{\text{AB}}]. \quad (\text{A1})$$

Let us introduce further auxilliary measurement operators

$$M_{a|x}^{(i)} = \sum_{\mathbf{a}, a_i=a} M_{\mathbf{a}|x} \quad N_{b|y}^{(i)} = \sum_{\mathbf{b}, b_i=b} N_{\mathbf{b}|y}. \quad (\text{A2})$$

With $M'_{a|x}$ we simply denote the reference single qudit measurements. Since we extract the tensor product of the reference state into the ancillary Hilbert space, to ease keeping track of the number of the extracted reference states we denote the Hilbert spaces of ancillary systems with A_j and B_j (instead of A' and B' in the main text). In order to relax the notation when writing measurement operators we omit the Hilbert space notation. Thus, we employ the following notation: $M_{a|x}^{(i)} \equiv M_{a|x}^{(i)A}$, $M_{\mathbf{a}|x} \equiv M_{\mathbf{a}|x}^A$, $N_{b|y}^{(i)} \equiv N_{b|y}^{(i)B}$, $N_{\mathbf{b}|y} \equiv N_{\mathbf{b}|y}^B$ for physical measurements and $M'_{a|x} \equiv M'_{a|x}^{A_j}$, $N'_{b|y} \equiv N'_{b|y}^{B_j}$ for reference measurements.

We prove the theorem by using mathematical induction. In the first step we prove the base case, *i.e.* that the theorem holds when $n = 1$. In the second step we prove the so-called inductive step, saying that if the theorem holds for some natural number i it also holds for $i + 1$. The whole theorem is proven by demonstrating the correctness of the base and the inductive step. The validity of the base step holds trivially since the theorem assumes that the Bell inequality under consideration is self-testing. The condition $\mathcal{I}_1 = \beta$ implies the existence of the local unitary $U_1 = U_{AA_1} \otimes U_{BB_1} \otimes \mathbb{1}_P$ such that

$$U_1 |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} = |\xi_1\rangle^{\text{ABP}} \otimes |\psi'\rangle^{A_1 B_1} \quad (\text{A3})$$

$$U_1 M_{a|x}^{(1)} \otimes N_{b|y}^{(1)} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} = |\xi_1\rangle^{\text{ABP}} \otimes \left(M'_{a|x}^{A_1} \otimes N'_{b|y}^{B_1} \right) |\psi'\rangle^{A_1 B_1} \quad (\text{A4})$$

To start the inductive step assume that the theorem holds for i , *i.e.* that $\sum_{\mathbf{a}_{i-1} \mathbf{b}_{i-1}} \mathcal{I}_{\mathbf{a}_{i-1} \mathbf{b}_{i-1}}^i = o^{2(i-1)} \beta$ implies there exist the local unitary $U_i = U_{AA_1 \dots A_i} \otimes U_{BB_1 \dots B_i} \otimes \mathbb{1}_P$ such that

$$U_i |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} \dots \otimes |00\rangle^{A_i B_i} = |\xi_i\rangle^{\text{ABP}} \otimes |\psi'\rangle^{A_1 B_1} \otimes \dots \otimes |\psi'\rangle^{A_i B_i}, \quad (\text{A5})$$

$$U_i M_{\mathbf{a}_i|x} \otimes N_{\mathbf{b}_i|y} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} \dots \otimes |00\rangle^{A_i B_i} = |\xi_i\rangle^{\text{ABP}} \bigotimes_{j=1}^i M'_{a_j|x} \otimes N'_{b_j|y} |\psi'\rangle^{A_j B_j}. \quad (\text{A6})$$

By summing (A6) over \mathbf{b}_i and using the completeness relation $\sum_{\mathbf{b}_i} N_{\mathbf{b}_i|y} = \mathbb{1}$ we obtain

$$U_i M_{\mathbf{a}_i|x} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} \dots \otimes |00\rangle^{A_i B_i} = |\xi_i\rangle^{\text{ABP}} \bigotimes_{j=1}^i M'_{a_j|x} \otimes \mathbb{1}^{B_j} |\psi'\rangle^{A_j B_j},$$

which can be rewritten as

$$\begin{aligned} \left(U_{AA_1 \dots A_i} M_{\mathbf{a}_i|x} \otimes \mathbb{1}^{A_1 \dots A_i} U_{AA_1 \dots A_i}^\dagger \right) U_i |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1} \dots \otimes |00\rangle^{A_i B_i} = \\ = |\xi_i\rangle^{\text{ABP}} \bigotimes_{j=1}^i M'_{a_j|x} \otimes \mathbb{1}^{B_j} |\psi'\rangle^{A_j B_j}. \end{aligned} \quad (\text{A7})$$

By comparing (A7) and (A5) we obtain

$$U_{AA_1 \dots A_i} M_{\mathbf{a}_i|x} \otimes \mathbb{1}^{A_1 \dots A_i} U_{AA_1 \dots A_i}^\dagger = S_{\mathbf{a}_i|x}^A \otimes M'_{\mathbf{a}_i|x}^{A_1 \dots A_i} \quad (\text{A8})$$

where $S_{\mathbf{a}_i|x} |\xi_i\rangle = |\xi_i\rangle$ for all \mathbf{a}_i and x . Note that A8 is correct in case $\text{tr}_{B_1 \dots B_i} |\psi'\rangle\langle\psi'|$ is full rank. We make assumption that this is indeed the case, which is a standard assumption in the self-testing scenarios. Since $U_{AA_1 \dots A_i}$ preserves the identity the condition

$$\sum_{\mathbf{a}_i} S_{\mathbf{a}_i|x}^A \otimes M'_{\mathbf{a}_i|x}^{A_1 \dots A_i} = \mathbb{1}^A \otimes \mathbb{1}^{A_1 \dots A_i} \quad (\text{A9})$$

must be satisfied. Since $\sum_{\mathbf{a}_i} M'_{\mathbf{a}_i|x} = \mathbb{1}$, the condition is satisfied if and only if $S_{\mathbf{a}_i|x} = \mathbb{1}$ for all \mathbf{a}_i and x . This can be seen through the simple reasoning. $U_{i,A} \equiv U_{AA_1 \dots A_i}$ is unitary and thus $\mathbb{1} \geq S_{\mathbf{a}_i|x}^A \otimes M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i} \geq 0$. Hence, for arbitrary quantum states ρ^A and $\tau^{A_1 \dots A_i}$ it holds $\text{tr}(S_{\mathbf{a}_i|x}^A \rho) = \alpha_i$ and $\text{tr}(M'_{\mathbf{a}_i|x} \tau) = \beta_i$ where $0 \leq \alpha_i, \beta_i \leq 1$. Eq. (A9) implies $\sum_i \alpha_i \beta_i = 1$ and the completeness of $M'_{\mathbf{a}_i|x}$ implies $\sum_i \beta_i = 1$. Thus, it also holds $\sum_i (1 - \alpha_i) \beta_i = 0$. The sum of nonnegative numbers is equal to zero if and only if each of them is equal to zero. Since the argumentation must hold for all states it implies $S_{\mathbf{a}_i|x} = \mathbb{1}$ for all \mathbf{a}_i and x . Eq. (A8) reduces to

$$U_{AA_1 \dots A_i} M_{\mathbf{a}_i|x} \otimes \mathbb{1}^{A_1 \dots A_i} U_{AA_1 \dots A_i}^\dagger = \mathbb{1}^A \otimes M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i} \quad (\text{A10})$$

for all \mathbf{a}_i and x . Analogous conclusion can be obtained for Bob's operators

$$U_{BB_1 \dots B_i} N_{\mathbf{b}_i|x} \otimes \mathbb{1}^{B_1 \dots B_i} U_{BB_1 \dots B_i}^\dagger = \mathbb{1}^B \otimes N'_{\mathbf{b}_i|x}{}^{B_1 \dots B_i} \quad (\text{A11})$$

for all \mathbf{b}_i and y . Note now that $M_{\mathbf{a}_i|x} = \sum_{a_{i+1}} M_{\mathbf{a}_i, a_{i+1}|x}$, where \mathbf{a}_i, a_{i+1} is just a different way to write \mathbf{a}_{i+1} , where $(i+1)$ -th output is separately written, as to be able to keep track of it. Similar eq. holds for Bob and thus eqs. (A10) and (A11) imply:

$$U_{AA_1 \dots A_i} M_{\mathbf{a}_i, a_{i+1}|x}^A \otimes \mathbb{1}^{A_1 \dots A_i} U_{AA_1 \dots A_i}^\dagger = K_{\mathbf{a}_i, a_{i+1}|x}^A \otimes M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i}, \quad (\text{A12})$$

$$U_{BB_1 \dots B_i} N_{\mathbf{b}_i, b_{i+1}|y}^B \otimes \mathbb{1}^{B_1 \dots B_i} U_{BB_1 \dots B_i}^\dagger = L_{\mathbf{b}_i, b_{i+1}|y}^B \otimes N'_{\mathbf{b}_i|y}{}^{B_1 \dots B_i}, \quad (\text{A13})$$

where operators $K_{\mathbf{a}_i, a_{i+1}|x}$ and $L_{\mathbf{b}_i, b_{i+1}|y}$ satisfy

$$\sum_{a_{i+1}} K_{\mathbf{a}_i, a_{i+1}|x} = \mathbb{1}, \quad \sum_{b_{i+1}} L_{\mathbf{b}_i, b_{i+1}|y} = \mathbb{1}. \quad (\text{A14})$$

We prove that the operators on the r.h.s. of equalities (A12) and (A13) have the tensor product structure by reductio ab absurdum. Assume $U_{AA_1 \dots A_i} M_{\mathbf{a}_i, a_{i+1}|x}^A \otimes \mathbb{1}^{A_1 \dots A_i} U_{AA_1 \dots A_i}^\dagger \equiv \tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i}$ are entangled across the bipartition $A|A_1 \dots A_i$. Then the following equation holds:

$$\sum_{a_{i+1}} \tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i} = \mathbb{1}^A \otimes M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i} \quad (\text{A15})$$

Let us denote $\text{tr}_A [\tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i}] = k_{a_{i+1}} \bar{K}_{\mathbf{a}_{i+1}}^{A_1 \dots A_i}$, where $\bar{K}_{\mathbf{a}_{i+1}}^{A_1 \dots A_i} \geq 0$. Given that $\tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i}$ is positive for all \mathbf{a}_{i+1} , we have that $k_{a_{i+1}} \geq 0$ for all a_{i+1} . By tracing out the Hilbert space A in eq. (A15) we obtain

$$\sum_{a_{i+1}} \frac{k_{a_{i+1}}}{D} \bar{K}_{\mathbf{a}_{i+1}}^{A_1 \dots A_i} = M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i}, \quad (\text{A16})$$

where D is the dimension of Hilbert space \mathcal{H}_A . Since $M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i}$ is, by assumption, a tensor product of rank-one projectors, eq. (A16) implies $\bar{K}_{\mathbf{a}_{i+1}}^{A_1 \dots A_i} = M'_{\mathbf{a}_i|x}{}^{A_1 \dots A_i}$ for all \mathbf{a}_i . Henceforth, we have $\text{tr}_A [\tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i}] = k_{a_{i+1}} M'_{\mathbf{a}_{i+1}}{}^{A_1 \dots A_i}$, and as $M'_{\mathbf{a}_{i+1}}{}^{A_1 \dots A_i}$ is a rank-one projector, there cannot be entanglement in $\tilde{K}_{\mathbf{a}_{i+1}}^{AA_1 \dots A_i}$ across the bipartition $A|A_1 \dots A_i$, which justifies the form of eq. (A12). Similar argument holds for (A13).

Let us now write down the expression for the conditional Bell value

$$\mathcal{I}_{\mathbf{a}_i, \mathbf{b}_i}^{i+1} = \sum_{a_{i+1} b_{i+1} xy} \frac{b_{a_{i+1} b_{i+1}}^{xy}}{p(\mathbf{a}_i, \mathbf{b}_i|xy)} \text{tr} \left[\left(M_{\mathbf{a}_i, a_{i+1}|x} \otimes N_{\mathbf{b}_i, b_{i+1}|y} \right) \rho_{AB} \otimes |00\rangle\langle 00|^{A_1 B_1 \dots A_i B_i} \right], \quad (\text{A17})$$

where $b_{a_{i+1} b_{i+1}}^{xy}$ are the coefficients from the original Bell inequality corresponding to the probability $p(a_{i+1} b_{i+1}|xy)$. Given the self-testing statements (A5), (A12), (A13) it can be rewritten in the following

way

$$\mathcal{I}_{\mathbf{a}_i, \mathbf{b}_i}^{i+1} = \sum_{a_{i+1}b_{i+1}xy} \frac{b_{a_{i+1}b_{i+1}}^{xy}}{p(\mathbf{a}_i, \mathbf{b}_i|xy)} \text{tr} \left[\left(\mathbf{K}_{\mathbf{a}_i, a_{i+1}|x} \otimes \mathbf{L}_{\mathbf{b}_i, b_{i+1}|y} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \bigotimes_{j=1}^i \left(\left(\mathbf{M}'_{\mathbf{a}_i|x} \otimes \mathbf{N}'_{\mathbf{b}_i|y} \right) |\psi'\rangle\langle\psi'|^{A_j B_j} \right) \right]. \quad (\text{A18})$$

The expression can be further simplified

$$\mathcal{I}_{\mathbf{a}_i, \mathbf{b}_i}^{i+1} = \sum_{a_{i+1}b_{i+1}xy} \frac{b_{a_{i+1}b_{i+1}}^{xy}}{p(\mathbf{a}_i, \mathbf{b}_i|xy)} \text{tr} \left[\left(\mathbf{K}_{\mathbf{a}_i, a_{i+1}|x} \otimes \mathbf{L}_{\mathbf{b}_i, b_{i+1}|y} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \right] \prod_{j=1}^i \text{tr} \left[\left(\mathbf{M}'_{a_j|x} \otimes \mathbf{N}'_{b_j|y} \right) |\psi'\rangle\langle\psi'|^{A_j B_j} \right] \quad (\text{A19})$$

$$= \sum_{a_{i+1}b_{i+1}xy} b_{a_{i+1}b_{i+1}}^{xy} \text{tr} \left[\left(\mathbf{K}_{\mathbf{a}_i, a_{i+1}|x} \otimes \mathbf{L}_{\mathbf{b}_i, b_{i+1}|y} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \right]. \quad (\text{A20})$$

The equalities come from the property of trace $\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B)$ and observing that $p(\mathbf{a}_i, \mathbf{b}_i|xy) = \prod_{j=1}^i \text{tr} \left[\left(\mathbf{M}'_{a_j|x} \otimes \mathbf{N}'_{b_j|y} \right) |\psi'\rangle\langle\psi'|^{A_j B_j} \right]$. Let us now sum different conditional Bell values

$$\begin{aligned} \sum_{\mathbf{a}_i, \mathbf{b}_i} \mathcal{I}_{\mathbf{a}_i, \mathbf{b}_i}^{i+1} &= \sum_{\mathbf{a}_i, \mathbf{b}_i} \sum_{a_{i+1}b_{i+1}xy} b_{a_{i+1}b_{i+1}}^{xy} \text{tr} \left[\left(\mathbf{K}_{\mathbf{a}_i, a_{i+1}|x} \otimes \mathbf{L}_{\mathbf{b}_i, b_{i+1}|y} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \right] \\ &= o^{2i} \sum_{a_{i+1}b_{i+1}xy} b_{a_{i+1}b_{i+1}}^{xy} \text{tr} \left[\left(\mathbf{K}_{a_{i+1}|x}^{(i+1)} \otimes \mathbf{L}_{b_{i+1}|y}^{(i+1)} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \right], \end{aligned} \quad (\text{A21})$$

where we introduced new operators

$$o^i \mathbf{K}_{a_{i+1}|x}^{(i+1)} = \sum_{\mathbf{a}_i} \mathbf{K}_{\mathbf{a}_i, a_{i+1}|x}, \quad o^i \mathbf{L}_{b_{i+1}|y}^{(i+1)} = \sum_{\mathbf{b}_i} \mathbf{L}_{\mathbf{b}_i, b_{i+1}|y}. \quad (\text{A22})$$

Note that $\mathbf{K}_{a_{i+1}|x}^{(i+1)}$ and $\mathbf{L}_{b_{i+1}|y}^{(i+1)}$ are positive and satisfy the completeness relations $\sum_{a_{i+1}} \mathbf{K}_{a_{i+1}|x}^{(i+1)} = \mathbb{1}$ and $\sum_{b_{i+1}} \mathbf{L}_{b_{i+1}|y}^{(i+1)} = \mathbb{1}$ (see eq. (A14)). Hence they represent valid quantum measurements. The condition for self-testing is $\mathcal{J}^i = \beta$ for all i , which through the definition of \mathcal{J}^i given in eq. (5) implies $\sum_{\mathbf{a}_i, \mathbf{b}_i} \mathcal{I}_{\mathbf{a}_i, \mathbf{b}_i}^{i+1} = o^{2i} \beta$, or equivalently

$$\sum_{a_{i+1}b_{i+1}xy} b_{a_{i+1}b_{i+1}}^{xy} \text{tr} \left[\left(\mathbf{K}_{a_{i+1}|x}^{(i+1)} \otimes \mathbf{L}_{b_{i+1}|y}^{(i+1)} \right) |\xi_i\rangle\langle\xi_i|^{\text{ABP}} \right] = \beta. \quad (\text{A23})$$

Since the Bell inequality is self-testing the reference experiment the eq. (A23) implies the existence of the local unitary transformation $U'_{i+1} = U'_{AA_{i+1}} \otimes U'_{BB_{i+1}} \otimes \mathbb{1}_P$ such that

$$U'_{i+1} |\xi_i\rangle^{\text{ABP}} \otimes |00\rangle^{A_{i+1}B_{i+1}} = |\xi_{i+1}\rangle^{\text{ABP}} \otimes |\psi'\rangle^{A_{i+1}B_{i+1}} \quad (\text{A24})$$

$$U'_{i+1} \left[\mathbf{K}_{a_{i+1}|x}^{(i+1)} \otimes \mathbf{L}_{b_{i+1}|y}^{(i+1)} |\xi_i\rangle^{\text{ABP}} \otimes |00\rangle^{A_{i+1}B_{i+1}} \right] = |\xi_{i+1}\rangle^{\text{ABP}} \otimes \left(\mathbf{M}'_{a_{i+1}|x}^{A_{i+1}} \otimes \mathbf{N}'_{b_{i+1}|y}^{B_{i+1}} \right) |\psi'\rangle^{A_{i+1}B_{i+1}} \quad (\text{A25})$$

Combining eqs (A24)-(A25) with (A5)-(A6) leads to the parallel self-testing of $\bigotimes_{j=1}^{i+1} |\psi'\rangle$:

$$U'_{i+1} \left[U_i \left[|\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1 \dots A_i B_i} \right] \otimes |00\rangle^{A_{i+1} B_{i+1}} \right] = |\xi_{i+1}\rangle^{\text{ABP}} \bigotimes_{j=1}^{i+1} |\psi'\rangle^{A_j B_j} \quad (\text{A26})$$

$$U'_{i+1} \left[U_i \left[\mathbf{M}_{\mathbf{a}_i|x} \otimes \mathbf{N}_{\mathbf{b}_i|y} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{A_1 B_1 \dots A_i B_i} \right] \otimes |00\rangle^{A_{i+1} B_{i+1}} \right] = |\xi_{i+1}\rangle^{\text{ABP}} \otimes \left(\mathbf{M}'_{\mathbf{a}_i|x} \otimes \mathbf{N}'_{\mathbf{b}_i|y} \bigotimes_{j=1}^i |\psi'\rangle^{A_j B_j} \right) \otimes |\psi'\rangle \quad (\text{A27})$$

Now the aim is to self-test the action of measurements $M_{\mathbf{a}_{i+1}|x}$ and $N_{\mathbf{b}_{i+1}|y}$. Let us verify how the isometry $U'_{i+1} \circ U_i$ acts on these measurements. By using eqs. (A5), (A6), (A12) and (A13) we obtain:

$$\begin{aligned} U'_{i+1} \left[U_i \left[M_{\mathbf{a}_{i+1}|x} \otimes N_{\mathbf{b}_{i+1}|y} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1 \dots \text{A}_i\text{B}_i} \right] \otimes |00\rangle^{\text{A}_{i+1}\text{B}_{i+1}} \right] &= \\ &= U'_{i+1} \left[\left(K_{\mathbf{a}_{i+1}|x} \otimes L_{\mathbf{b}_{i+1}|y} |\xi_i\rangle^{\text{AB}} \right) \otimes \left(M'_{\mathbf{a}_i|x} \otimes N'_{\mathbf{b}_i|y} \bigotimes_{j=1}^i |\psi'\rangle^{\text{A}_j\text{B}_j} \right) \otimes |00\rangle^{\text{A}_{i+1}\text{B}_{i+1}} \right] \end{aligned} \quad (\text{A28})$$

Eq. (A25) implies $U'_{\text{AA}_{i+1}} \left[K_{\mathbf{a}_{i+1}|x} \otimes \mathbb{1}^{\text{A}_{i+1}} \right] U'^{\dagger}_{\text{AA}_{i+1}} = \mathbb{1}^{\text{A}} \otimes M'^{\text{A}_{i+1}}_{\mathbf{a}_{i+1}|x}$, similarly to the derivation of eq. (A10). Following the procedure used to prove eq. (A12), this implies $U'_{\text{AA}_{i+1}} \left[K_{\mathbf{a}_{i+1}|x} \otimes \mathbb{1}^{\text{A}_{i+1}} \right] U'^{\dagger}_{\text{AA}_{i+1}} = \bar{K}_{\mathbf{a}_{i+1}|x} \otimes M'^{\text{A}_{i+1}}_{\mathbf{a}_{i+1}|x}$ and $U'_{\text{BB}_{i+1}} \left[L_{\mathbf{b}_{i+1}|y} \otimes \mathbb{1}^{\text{B}_{i+1}} \right] U'^{\dagger}_{\text{BB}_{i+1}} = \bar{L}_{\mathbf{b}_{i+1}|y} \otimes N'^{\text{B}_{i+1}}_{\mathbf{b}_{i+1}|y}$, where $\bar{K}_{\mathbf{a}_{i+1}|x}$ and $\bar{L}_{\mathbf{b}_{i+1}|y}$ are positive operators. The eq. (A27) can be rewritten as

$$\begin{aligned} U'_{i+1} \circ U_i \left[M_{\mathbf{a}_i|x} \otimes N_{\mathbf{b}_i|y} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1 \dots \text{A}_{i+1}\text{B}_{i+1}} \right] &= U'_{i+1} \circ U_i \left[\left(\sum_{\mathbf{a}_{i+1}} M_{\mathbf{a}_i\mathbf{a}_{i+1}|x} \otimes \sum_{\mathbf{b}_{i+1}} N_{\mathbf{b}_i\mathbf{b}_{i+1}|y} |\psi\rangle^{\text{ABP}} \right) \otimes |00\rangle^{\text{A}_{i+1}\text{B}_{i+1}} \right] \\ &= U'_{i+1} \left[\left(\sum_{\mathbf{a}_{i+1}} K_{\mathbf{a}_i\mathbf{a}_{i+1}|x} \otimes \sum_{\mathbf{b}_{i+1}} L_{\mathbf{b}_i\mathbf{b}_{i+1}|y} |\xi_i\rangle^{\text{ABP}} \right) \otimes \left(M'_{\mathbf{a}_i|x} \otimes N'_{\mathbf{b}_i|y} \bigotimes_{j=1}^i |\psi'\rangle^{\text{A}_j\text{B}_j} \right) \otimes |00\rangle^{\text{A}_{i+1}\text{B}_{i+1}} \right] \\ &= \sum_{\mathbf{a}_{i+1}, \mathbf{b}_{i+1}} \left(\bar{K}_{\mathbf{a}_i, \mathbf{a}_{i+1}|x} \otimes \bar{L}_{\mathbf{b}_i, \mathbf{b}_{i+1}|y} |\xi_{i+1}\rangle^{\text{ABP}} \right) \otimes \left(M'_{\mathbf{a}_i|x} \otimes N'_{\mathbf{b}_i|y} \bigotimes_{j=1}^i |\psi'\rangle^{\text{A}_j\text{B}_j} \right) \otimes \left(M'_{\mathbf{a}_{i+1}|x} \otimes N'_{\mathbf{b}_{i+1}|y} |\psi'\rangle^{\text{A}_{i+1}\text{B}_{i+1}} \right) \end{aligned}$$

The second equality is the consequence of eqs. (A5), (A12) and (A13), while the third equality comes from $U'_{\text{AA}_{i+1}} \left[K_{\mathbf{a}_{i+1}|x} \otimes \mathbb{1}^{\text{A}_{i+1}} \right] U'^{\dagger}_{\text{AA}_{i+1}} = \bar{K}_{\mathbf{a}_{i+1}|x} \otimes M'^{\text{A}_{i+1}}_{\mathbf{a}_{i+1}|x}$ and analogously for $L_{\mathbf{b}_{i+1}|y}$. The final equation is equivalent to (A27) if and only if $\bar{K}_{\mathbf{a}_i, \mathbf{a}_{i+1}|x} = \bar{L}_{\mathbf{b}_i, \mathbf{b}_{i+1}|y} = \mathbb{1}$ for all $\mathbf{a}_{i+1}, \mathbf{b}_{i+1}, x, y$. This can be proven by using the same argumentation used after eq. (A9) given that $0 \leq \bar{K}_{\mathbf{a}_i, \mathbf{a}_{i+1}|x}, \bar{L}_{\mathbf{b}_i, \mathbf{b}_{i+1}|y} \leq 1$ and $\sum_{\mathbf{a}_{i+1}} M'_{\mathbf{a}_{i+1}|x} = \mathbb{1}, \sum_{\mathbf{b}_{i+1}} N'_{\mathbf{b}_{i+1}|y} = \mathbb{1}$.

Hence, by denoting $U_{i+1} = U'_{i+1} \circ U_i$, we reduce eq. (A28) to

$$U_{i+1} \left[M_{\mathbf{a}_{i+1}|x} \otimes N_{\mathbf{b}_{i+1}|y} |\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1 \dots \text{A}_{i+1}\text{B}_{i+1}} \right] = |\xi_{i+1}\rangle^{\text{ABP}} \otimes \left(\bigotimes_{j=1}^{i+1} M'_{\mathbf{a}_j|x} \otimes N'_{\mathbf{b}_j|y} |\psi'\rangle^{\text{A}_j\text{B}_j} \right) \quad (\text{A29})$$

With this we have proved the inductive step, and with it completed the theorem proof.

B Example: parallel self-testing beyond Bell inequalities

In this section we give example of lifting the self-testing protocol which is based not on the maximal violation of a Bell inequality but reproduction of the whole set of correlations. For the sake of simplicity we chose the self-testing protocol in the simplest scenario with two parties, each performing two binary measurements ((2,2,2) scenario). The self-testing correlations are

$$\langle \psi | A_0 \otimes B_0 | \psi \rangle = \cos \gamma, \quad \langle \psi | A_0 \otimes B_1 | \psi \rangle = -\cos \delta, \quad (\text{B30})$$

$$\langle \psi | A_1 \otimes B_0 | \psi \rangle = \sin \gamma, \quad \langle \psi | A_1 \otimes B_1 | \psi \rangle = \sin \delta, \quad (\text{B31})$$

for $\gamma \neq \delta$ and $\gamma, \delta \in (0, \pi/4]$. A_i and B_j are observables defined as $A_i = M_{0|i} - M_{1|i}$ and $B_i = N_{0|i} - N_{1|i}$. In [WWS16] it is proven that this set of correlations self-tests the maximally entangled pair of qubits. The reference measurement observables are

$$\begin{aligned} A'_0 &= \sigma_Z, & A'_1 &= \sigma_X, \\ B'_0 &= \cos \gamma \sigma_Z + \sin \gamma \sigma_X, & B'_1 &= \cos \delta \sigma_Z - \sin \delta \sigma_X. \end{aligned}$$

We omit the self-testing proof here and direct reader's attention to [WWS16]. The isometry used in the proof is the Swap isometry U and physical experiment reproducing correlations (B30)-(B31) satisfies the following equations

$$U \left[|\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1} \right] = |\xi\rangle^{\text{ABP}} \otimes |\phi^+\rangle^{\text{A}_1\text{B}_1}, \quad (\text{B32})$$

$$U \left[(\mathbf{M}_{a|x} \otimes \mathbf{N}_{b|y} |\psi\rangle^{\text{ABP}}) \otimes |00\rangle^{\text{A}_1\text{B}_1} \right] = |\xi\rangle^{\text{ABP}} \otimes (\mathbf{M}'_{a|x} \otimes \mathbf{N}'_{b|y} |\phi^+\rangle^{\text{A}_1\text{B}_1}). \quad (\text{B33})$$

Note that one might show that correlations (B30)-(B31) maximally violate some Bell inequality and the procedure corresponding to the Theorem 1 can be applied to build a self-testing protocol for a tensor product of n maximally entangled qubit pairs. However, we still find it useful to show how to deal with a self-testing protocol based on the reproduction of the whole set of correlations. In $(2, 2, 2)$ case one can use standard methods to find the Bell inequality maximally violated by some extremal point of the set of quantum correlations (for example NPA hierarchy methods [NPA07, NPA08]), but in more complicated scenarios this might not be an easy task. Furthermore, most of the known self-testing protocols for multipartite states are not based on the maximal Bell inequality violation.

In what follows we show how to use the above given self-test to build another self-test, using the same number of measurement choices, certifying $|\phi^+\rangle \otimes |\phi^+\rangle$. Let us introduce the following notation

$$\mathbf{A}_x^{(k)} = \sum_{\mathbf{a}} (-1)^{a_k} \mathbf{M}_{\mathbf{a}|x}, \quad \mathbf{B}_y^{(k)} = \sum_{\mathbf{b}} (-1)^{b_k} \mathbf{N}_{\mathbf{b}|y}, \quad \text{for } k = 1, 2. \quad (\text{B34})$$

The condition for self-testing in this case is reproduction of the following correlations:

$$\langle \psi | \mathbf{A}_0^{(1)} \otimes \mathbf{B}_0^{(1)} | \psi \rangle = \cos \gamma, \quad \langle \psi | \mathbf{A}_0^{(1)} \otimes \mathbf{B}_1^{(1)} | \psi \rangle = -\cos \delta, \quad (\text{B35})$$

$$\langle \psi | \mathbf{A}_1^{(1)} \otimes \mathbf{B}_0^{(1)} | \psi \rangle = \sin \gamma, \quad \langle \psi | \mathbf{A}_1^{(1)} \otimes \mathbf{B}_1^{(1)} | \psi \rangle = \sin \delta \quad (\text{B36})$$

$$\frac{1}{p(a_1 = a, b_1 = b|00)} \langle \psi | (\mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)}) (\mathbf{A}_0^{(2)} \otimes \mathbf{B}_0^{(2)}) (\mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)}) | \psi \rangle = \cos \gamma, \quad \forall a, b \quad (\text{B37})$$

$$\frac{1}{p(a_1 = a, b_1 = b|01)} \langle \psi | (\mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|1}^{(1)}) (\mathbf{A}_0^{(2)} \otimes \mathbf{B}_1^{(2)}) (\mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|1}^{(1)}) | \psi \rangle = -\cos \delta, \quad \forall a, b \quad (\text{B38})$$

$$\frac{1}{p(a_1 = a, b_1 = b|10)} \langle \psi | (\mathbf{M}_{a|1}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)}) (\mathbf{A}_1^{(2)} \otimes \mathbf{B}_0^{(2)}) (\mathbf{M}_{a|1}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)}) | \psi \rangle = \sin \gamma, \quad \forall a, b \quad (\text{B39})$$

$$\frac{1}{p(a_1 = a, b_1 = b|11)} \langle \psi | (\mathbf{M}_{a|1}^{(1)} \otimes \mathbf{N}_{b|1}^{(1)}) (\mathbf{A}_1^{(2)} \otimes \mathbf{B}_1^{(2)}) (\mathbf{M}_{a|1}^{(1)} \otimes \mathbf{N}_{b|1}^{(1)}) | \psi \rangle = \sin \delta, \quad \forall a, b. \quad (\text{B40})$$

In terms just of the observed probabilities the set of conditions (B35)-(B40) can be written as

$$p(a_1 = b_1|00) - p(a_1 \neq b_1|00) = \cos \gamma, \quad p(a_1 = b_1|01) - p(a_1 \neq b_1|01) = -\cos \delta, \quad (\text{B41})$$

$$p(a_1 = b_1|10) - p(a_1 \neq b_1|10) = \sin \gamma, \quad p(a_1 = b_1|11) - p(a_1 \neq b_1|11) = \cos \delta, \quad (\text{B42})$$

$$(p(a_2 = b_2|x = 0, y = 0, a_1 = a, b_1 = b) - p(a_2 \neq b_2|x = 0, y = 0, a_1 = a, b_1 = b)) = \cos \gamma, \quad \forall a, b \quad (\text{B43})$$

$$(p(a_2 = b_2|x = 0, y = 1, a_1 = a, b_1 = b) - p(a_2 \neq b_2|x = 0, y = 1, a_1 = a, b_1 = b)) = -\cos \delta, \quad \forall a, b \quad (\text{B44})$$

$$(p(a_2 = b_2|x = 1, y = 0, a_1 = a, b_1 = b) - p(a_2 \neq b_2|x = 1, y = 0, a_1 = a, b_1 = b)) = \sin \gamma, \quad \forall a, b \quad (\text{B45})$$

$$(p(a_2 = b_2|x = 1, y = 1, a_1 = a, b_1 = b) - p(a_2 \neq b_2|x = 1, y = 1, a_1 = a, b_1 = b)) = \sin \delta, \quad \forall a, b. \quad (\text{B46})$$

The proof goes along the same line as the proof of Theorem 1. Equations (B35)-(B36) imply the existence of the isometry $U_1 = U_{\text{AA}_1} \otimes U_{\text{BB}_1} \otimes \mathbb{1}_{\text{P}}$ such that

$$U_1 \left(|\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1} \right) = |\xi_1\rangle^{\text{ABP}} \otimes |\phi^+\rangle^{\text{A}_1\text{B}_1}, \quad (\text{B47})$$

$$U_1 \left((\mathbf{M}_{a|x}^{(1)} \otimes \mathbf{N}_{b|y}^{(1)} |\psi\rangle^{\text{ABP}}) \otimes |00\rangle^{\text{A}_1\text{B}_1} \right) = |\xi_1\rangle^{\text{ABP}} \otimes (\mathbf{M}'_{a|x} \otimes \mathbf{N}'_{b|y} |\phi^+\rangle^{\text{A}_1\text{B}_1}). \quad (\text{B48})$$

These two equations imply the following set of equations

$$U_{AA_1} \left(\mathbf{M}_{a|x}^{(1)} \otimes \mathbb{1}^{A_1} \right) U_{AA_1}^\dagger = \mathbb{1}^A \otimes \mathbf{M}'_{a|x}{}^{A_1}, \quad U_{BB_1} \left(\mathbf{N}_{b|y}^{(1)} \otimes \mathbb{1}^{B_1} \right) U_{BB_1}^\dagger = \mathbb{1}^B \otimes \mathbf{N}'_{b|y}{}^{B_1}, \quad (\text{B49})$$

$$U_{AA_1} \left(\mathbf{M}_{a_1, a_2|x} \otimes \mathbb{1}^{A_1} \right) U_{AA_1}^\dagger = \mathbf{K}_{a_1, a_2|x}^A \otimes \mathbf{M}'_{a_1|x}{}^{A_1}, \quad U_{BB_1} \left(\mathbf{N}_{b_1, b_2|y} \otimes \mathbb{1}^{B_1} \right) U_{BB_1}^\dagger = \mathbf{L}_{b_1, b_2|y}^B \otimes \mathbf{N}'_{b_1|y}{}^{B_1}, \quad (\text{B50})$$

where the operators $\mathbf{K}_{a_1, a_2|x}$, $\mathbf{L}_{b_1, b_2|y}$ are positive semidefinite and satisfy

$$\sum_{a_2} \mathbf{K}_{a_1, a_2|x} = \mathbb{1}, \quad \sum_{b_2} \mathbf{L}_{b_1, b_2|y} = \mathbb{1} \quad (\text{B51})$$

Given all these equations the first expression from (B37) can be rewritten as

$$\begin{aligned} & \frac{1}{p(a_1 = a, b_1 = b|00)} \text{tr} \left[(A_0^{(2)} \otimes B_0^{(2)}) (\mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)} |\psi\rangle\langle\psi| \mathbf{M}_{a|0}^{(1)} \otimes \mathbf{N}_{b|0}^{(1)}) \right] = \\ & = \frac{1}{p(a_1 = a, b_1 = b|00)} \text{tr} \left[U \left(A_0^{(2)} \otimes B_0^{(2)} \right) U^\dagger |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \otimes (\mathbf{M}'_{a|0} \otimes \mathbf{N}'_{b|0} |\phi^+\rangle\langle\phi^+|^{\text{A}_1\text{B}_1} \mathbf{M}'_{a|0} \otimes \mathbf{N}'_{b|0}) \right] = \end{aligned} \quad (\text{B52})$$

$$\begin{aligned} & = \frac{1}{p_1(a_1 = a, b_1 = b|00)} \sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|0} \otimes \mathbf{L}_{b, b_2|0}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \otimes (\mathbf{M}'_{a|0} \otimes \mathbf{N}'_{b|0} |\phi^+\rangle\langle\phi^+|^{\text{A}_1\text{B}_1}) \right] \\ & = \frac{1}{p(a_1 = a, b_1 = b|00)} \sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|0} \otimes \mathbf{L}_{b, b_2|0}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \right] \text{tr} \left[(\mathbf{M}'_{a|0} \otimes \mathbf{N}'_{b|0}) |\phi^+\rangle\langle\phi^+|^{\text{A}_1\text{B}_1} \right] \\ & = \sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|0} \otimes \mathbf{L}_{b, b_2|0}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \right] = \cos \gamma. \end{aligned} \quad (\text{B53})$$

This equation holds for all $a, b \in 0, 1$. Analogous equations can be obtain starting from the other three relations from (B37)-(B39):

$$\sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|0} \otimes \mathbf{L}_{b, b_2|1}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \right] = -\cos \delta \quad (\text{B54})$$

$$\sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|1} \otimes \mathbf{L}_{b, b_2|0}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \right] = \sin \gamma \quad (\text{B55})$$

$$\sum_{a_2 b_2} (-1)^{a_2+b_2} \text{tr} \left[(\mathbf{K}_{a, a_2|1} \otimes \mathbf{L}_{b, b_2|1}) |\xi_1\rangle\langle\xi_1|^{\text{ABP}} \right] = \sin \delta. \quad (\text{B56})$$

Let us now introduce new operators

$$2\bar{A}_x = \sum_{a_1, a_2} (-1)^{a_2} \mathbf{K}_{a_1, a_2|x}, \quad 2\bar{B}_y = \sum_{b_1, b_2} (-1)^{b_2} \mathbf{L}_{b_1, b_2|y} \quad (\text{B57})$$

which are valid measurements observables (cf. (B51)). Since eqs. (B53), (B54), (B55) and (B56) hold for all values of a and b by summing over all the different values we obtain

$$\langle \xi_1 | \bar{A}_0 \otimes \bar{B}_0 | \xi_1 \rangle = \cos \gamma, \quad \langle \xi_1 | \bar{A}_0 \otimes \bar{B}_1 | \xi_1 \rangle = -\cos \delta, \quad (\text{B58})$$

$$\langle \xi_1 | \bar{A}_1 \otimes \bar{B}_0 | \xi_1 \rangle = \sin \gamma, \quad \langle \xi_1 | \bar{A}_1 \otimes \bar{B}_1 | \xi_1 \rangle = \sin \delta \quad (\text{B59})$$

These relations are exactly self-testing ones and they imply the existence of a local unitary $U_2 = U_{AA_2} \otimes U_{BB_2} \otimes \mathbb{1}_P$ such that

$$U_2 \left[|\xi_1\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_2\text{B}_2} \right] = |\xi\rangle^{\text{ABP}} \otimes |\phi^+\rangle^{\text{A}_2\text{B}_2} \quad (\text{B60})$$

Combining this equation with (B47) we obtain

$$U_2 \circ U_1 \left[|\psi\rangle^{\text{ABP}} \otimes |0000\rangle^{\text{A}_1\text{A}_2\text{B}_1\text{B}_2} \right] = |\xi\rangle^{\text{ABP}} \otimes |\phi^+\rangle^{\text{A}_1\text{B}_1} \otimes |\phi^+\rangle^{\text{A}_2\text{B}_2}. \quad (\text{B61})$$

The proof for self-testing of measurements can be done in the same way as it is done in the proof of Theorem 1.

C Combining self-testing protocols to test a tensor product of different quantum states

Let us introduce the notion of compatible self-testing protocols, as those using the same number of inputs to self-tests the corresponding reference states. Here we outline how one can build a self-testing protocol certifying a tensor product of n different states, which can be independently self-tested by using compatible self-testing protocols.

Namely, the aim is to self-test a state of the form $\bigotimes_i |\psi'_i\rangle$, knowing that every $|\psi'_i\rangle$ can be self-tested through observing the maximal violation β_i of the inequality

$$\mathcal{I}_i \equiv \sum_{a_i, b_i=0}^{o_i-1} \sum_{x, y=0}^{m-1} b_{i, a_i b_i}^{xy} p_i(a_i b_i | xy) \leq \beta_i \quad (\text{C62})$$

Let us introduce the generalized conditional Bell value:

$$\mathcal{I}_{\mathbf{a}; \mathbf{b}_i}^{i+1} = \sum_{a_{i+1} b_{i+1} xy} \frac{b_{i+1, a_{i+1} b_{i+1}}^{xy}}{p(\mathbf{a}_i \mathbf{b}_i | xy)} \text{tr} \left[\left(\mathbf{M}_{\mathbf{a}_i, a_{i+1} | x} \otimes \mathbf{N}_{\mathbf{b}_i, b_{i+1} | y} \right) \rho_{AB} \otimes |00\rangle\langle 00|^{A_1 B_1 \dots A_i B_i} \right]. \quad (\text{C63})$$

The conditions for self-testing $\bigotimes_i |\psi'_i\rangle$ by using only m different inputs per party are the following

- $\mathcal{I}_1 = \beta_1$,
- $\sum_{\mathbf{a}; \mathbf{b}_i} \mathcal{I}_{\mathbf{a}; \mathbf{b}_i}^{i+1} = \left(\prod_{j=1}^i m_j \right)^2 \beta_{i+1}$.

The self-testing proof goes along the same lines as the proof for Theorem 1. The only difference is that for every i the second condition corresponds to the maximal violation of \mathcal{I}_i by the junk state appearing in the self-testing statement for $i - 1$.

D Proof of Theorem 4

In this section we give a proof of Theorem 4 which deals with combining two or more incompatible self-tests, *i.e.* self-tests corresponding to the scenarios with different inputs and/or output size. The general scenario is as follows: the protocol \mathcal{S}_i can be used to self-test the state $|\psi'_i\rangle$ in the scenario where each party has m_i inputs denoted with x_i, y_i and o_i outputs denoted as a_i, b_i . If the correlations $p_i(a_i b_i | x_i y_i)$ satisfy the self-testing conditions given by the protocol \mathcal{S}_i for each i then there is isometry mapping the physical state to the $\bigotimes_i |\psi'_i\rangle$. This can be seen as a generalization of parallel self-testing, where usually the reference state is an n -fold tensor product of some state.

According to the theorem conditions the state $|\psi'_i\rangle$, for $i \in \{1, \dots, n\}$, is self-tested through achieving the maximal violation of the Bell inequality \mathcal{I}_i , evaluated as

$$\mathcal{I}_i \equiv \sum_{a_i b_i x_i y_i} b_{i, a_i b_i}^{x_i y_i} p_i(a_i b_i | x_i y_i) = \beta_i. \quad (\text{D64})$$

The self-testing scenario is as follows: in every round Alice and Bob receive n classical inputs each, denoted with $\mathbf{x} = \{x_1, \dots, x_n\}$, $\mathbf{y} = \{y_1, \dots, y_n\}$, where $x_i, y_i \in \{0, 1, \dots, m_i - 1\}$. They return strings $\mathbf{a} = \{a_1, \dots, a_n\}$, $\mathbf{b} = \{b_1, \dots, b_n\}$, where $a_i, b_i \in \{0, 1, \dots, o_i - 1\}$. The measurement operators are denoted by $\mathbf{M}_{\mathbf{a} | \mathbf{x}}$ for Alice and $\mathbf{N}_{\mathbf{b} | \mathbf{y}}$ for Bob. Let us introduce the following notation

$$\mathbf{M}_{a_i | x_i} = \frac{1}{\prod_{j|j \neq i} m_j} \sum_{\mathbf{a}^{(i)}, \mathbf{x}^{(i)}} \mathbf{M}_{\mathbf{a} | \mathbf{x}}, \quad \mathbf{N}_{b_i | y_i} = \frac{1}{\prod_{j|j \neq i} m_j} \sum_{\mathbf{b}^{(i)}, \mathbf{y}^{(i)}} \mathbf{N}_{\mathbf{b} | \mathbf{y}} \quad (\text{D65})$$

These operators are valid measurement operators, as a sum of positive operators they are positive and they satisfy completeness relations $\sum_{a_i} M_{a_i|x_i} = \mathbb{1}$ and $\sum_{b_j} N_{b_j|y_j} = \mathbb{1}$, for all x_i and y_j . Let us define Bell-like expressions

$$\mathcal{I}_{\mathbf{x}^{(i)}\mathbf{y}^{(i)}}^i = \sum_{\mathbf{a}, \mathbf{b}, x_i, y_i} b_{i, a_i b_i}^{x_i y_i} p_i(\mathbf{a}|\mathbf{x}, \mathbf{y}) \quad (\text{D66})$$

The Bell violation for the i -th inequality is a normalized sum of values given in D66:

$$\mathcal{J}^i = \frac{1}{\prod_{j|j \neq i} m_j^2} \sum_{\mathbf{x}^{(i)}, \mathbf{y}^{(i)}} \mathcal{I}_{\mathbf{x}^{(i)}\mathbf{y}^{(i)}}^i, \quad (\text{D67})$$

Let us set $i = 1$. The Bell violation \mathcal{J}^1 can be modelled as

$$\mathcal{J}^1 = \sum_{a_1, b_1, x_1, y_1} b_{1, a_1 b_1}^{x_1 y_1} \langle \psi | M_{a_1|x_1} \otimes N_{b_1|y_1} | \psi \rangle \quad (\text{D68})$$

If the inequality \mathcal{J}^1 is maximally violated there exist a local unitary $U_1 = U_{AA_1} \otimes U_{BB_1} \otimes \mathbb{1}_P$ such that

$$U_1 \left[|\psi\rangle^{\text{ABP}} \otimes |00\rangle^{\text{A}_1\text{B}_1} \right] = |\xi_1\rangle^{\text{ABP}} \otimes |\psi'_1\rangle^{\text{A}_1\text{B}_1} \quad (\text{D69})$$

$$U_1 \left[\left(M_{a_1|x_1} \otimes N_{b_1|y_1} \otimes \mathbb{1}_P |\psi\rangle^{\text{ABP}} \right) \otimes |00\rangle^{\text{A}_1\text{B}_1} \right] = |\xi_1\rangle^{\text{ABP}} \otimes \left(M'_{a_1|x_1} \otimes N'_{b_1|y_1} |\psi'_1\rangle^{\text{A}_1\text{B}_1} \right). \quad (\text{D70})$$

This implies the following relations

$$U_{AA_1} \left[M_{a_1|x_1} \otimes \mathbb{1}^{\text{A}_1} \right] U_{AA_1}^\dagger = \mathbb{1}^{\text{A}} \otimes M'_{a_1|x_1}, \quad U_{BB_1} \left[N_{b_1|y_1} \otimes \mathbb{1}^{\text{B}_1} \right] U_{BB_1}^\dagger = \mathbb{1}^{\text{B}} \otimes N'_{b_1|y_1}, \quad (\text{D71})$$

$$U_{AA_1} \left[M_{a_1, a_2|x_1, x_2} \otimes \mathbb{1}^{\text{A}_1} \right] U_{AA_1}^\dagger = K_{a_1, a_2|x_1, x_2}^{\text{A}} \otimes M'_{a_1|x_1}, \quad U_{BB_1} \left[N_{b_1, b_2|y_1, y_2} \otimes \mathbb{1}^{\text{B}_1} \right] U_{BB_1}^\dagger = L_{b_1, b_2|y_1, y_2}^{\text{B}} \otimes N'_{b_1|y_1} \quad (\text{D72})$$

where

$$M_{a_1, a_2|x_1, x_2} = \frac{1}{m_3 m_4 \cdots m_n} \sum_{\substack{a_3, a_4, \dots, a_n \\ x_3, x_4, \dots, x_n}} M_{\mathbf{a}|\mathbf{x}} \quad N_{b_1, b_2|y_1, y_2} = \frac{1}{m_3 m_4 \cdots m_n} \sum_{\substack{b_3, b_4, \dots, b_n \\ y_3, y_4, \dots, y_n}} N_{\mathbf{b}|\mathbf{y}} \quad (\text{D73})$$

and $K_{a_1, a_2|x_1, x_2}$ and $L_{b_1, b_2|y_1, y_2}$ are positive operators satisfying

$$\sum_{a_2} K_{a_1, a_2|x_1, x_2} = \mathbb{1}, \quad \sum_{b_2} L_{b_1, b_2|y_1, y_2} = \mathbb{1}, \quad \text{for all } x_2, y_2, x_1, y_1, a_1, b_1 \quad (\text{D74})$$

In the second step the maximal violation of the inequality \mathcal{J}^2 can be modelled as

$$\mathcal{J}^2 = \frac{1}{m_1^2} \sum_{\substack{a_1, a_2, b_1, b_2 \\ x_1, x_2, y_1, y_2}} b_{2, a_2 b_2}^{x_2 y_2} \langle \psi | M_{a_1, a_2|x_1, x_2} \otimes N_{b_1, b_2|y_1, y_2} | \psi \rangle \quad (\text{D75})$$

$$= \frac{1}{m_1^2} \sum_{\substack{a_1, a_2, b_1, b_2 \\ x_1, x_2, y_1, y_2}} b_{2, a_2 b_2}^{x_2 y_2} \langle \xi_1 | K_{a_1, a_2|x_1, x_2} \otimes L_{b_1, b_2|y_1, y_2} | \xi_1 \rangle \langle \psi'_1 | M'_{a_1|x_1} \otimes N'_{b_1|y_1} | \psi'_1 \rangle \quad (\text{D76})$$

$$= \frac{1}{m_1^2} \sum_{a_1, b_1, x_1, y_1} \langle \psi'_1 | M'_{a_1|x_1} \otimes N'_{b_1|y_1} | \psi'_1 \rangle \sum_{a_2, b_2, x_2, y_2} b_{2, a_2 b_2}^{x_2 y_2} \langle \xi_1 | K_{a_1, a_2|x_1, x_2} \otimes L_{b_1, b_2|y_1, y_2} | \xi_1 \rangle \quad (\text{D77})$$

$$= \sum_{a_1, b_1, x_1, y_1} \frac{p_1(a_1, b_1|x_1, y_1)}{m_1^2} \sum_{a_2, b_2, x_2, y_2} b_{2, a_2 b_2}^{x_2 y_2} \langle \xi_1 | K_{a_1, a_2|x_1, x_2} \otimes L_{b_1, b_2|y_1, y_2} | \xi_1 \rangle \quad (\text{D78})$$

Since numbers $p_1(a_1 b_1 | x_1 y_1) / m_1^2$ are positive and sum to one, and all $K_{a_1, a_2 | x_1, x_2}$ and $L_{b_1, b_2 | y_1, y_2}$ are valid measurement operators the observation $\mathcal{J}^2 = \beta_2$ implies that

$$\sum_{a_2, b_2, x_2, y_2} b_{2, a_2 b_2}^{x_2 y_2} \langle \xi_1 | K_{a_1, a_2 | x_1, x_2} \otimes L_{b_1, b_2 | y_1, y_2} | \xi_1 \rangle = \beta_2 \quad (\text{D79})$$

for all a_1, b_1, x_1, y_1 . Let us define operators

$$K_{a_2 | x_2}^{(2)} = \frac{1}{m_1} \sum_{a_1, x_1} K_{a_1, a_2 | x_1, x_2}, \quad L_{b_2 | y_2}^{(2)} = \frac{1}{m_1} \sum_{b_1, y_1} L_{b_1, b_2 | y_1, y_2} \quad (\text{D80})$$

These operators are valid measurement operators, and they satisfy

$$\sum_{a_2, b_2, x_2, y_2} b_{2, a_2 b_2}^{x_2 y_2} \langle \xi_1 | K_{a_2 | x_2}^{(2)} \otimes L_{b_2 | y_2}^{(2)} | \xi_1 \rangle = \beta_2. \quad (\text{D81})$$

The maximal violation \mathcal{J}^2 implies that there exists a local unitary $U_2 = U_{AA_2} \otimes U_{BB_2} \otimes \mathbb{1}_P$ such that

$$U_2 \left[|\xi_1\rangle^{AB} \otimes |00\rangle^{A_2 B_2} \right] = |\xi_2\rangle^{AB} \otimes |\psi'_2\rangle^{A_2 B_2} \quad (\text{D82})$$

$$U_2 \left[(K_{a_2 | x_2}^{(2)} \otimes L_{b_2 | y_2}^{(2)} |\xi_1\rangle^{AB}) \otimes |00\rangle^{A_2 B_2} \right] = |\xi_2\rangle^{AB} \otimes (M'_{a_2 | x_2} \otimes N'_{b_2 | y_2} |\psi'_2\rangle^{A_2 B_2}). \quad (\text{D83})$$

Combining (D69) and (D82) we get a self-testing statement for a tensor product of two different states

$$U_2 \circ U_1 \left[|\psi\rangle^{ABP} \otimes |0000\rangle^{A_1 A_2 B_1 B_2} \right] = |\xi_2\rangle^{ABP} \otimes |\psi'_1\rangle^{A_1 B_1} \otimes |\psi'_2\rangle^{A_2 B_2}. \quad (\text{D84})$$

The process can be further repeated for $i = 3$ to $i = n$, reaching the final statement

$$U_n \circ \dots \circ U_1 \left[|\psi\rangle^{ABP} \otimes |0000\rangle^{A_1 \dots A_n B_1 \dots B_n} \right] = |\xi_n\rangle^{ABP} \otimes |\psi'_1\rangle^{A_1 B_1} \otimes \dots \otimes |\psi'_n\rangle^{A_n B_n}. \quad (\text{D85})$$