Robust self-testing of a singlet via the CHSH game

1 Introduction

Quantum entanglement forms a crucial component of many quantum information applications, including quantum key distribution (QKD), quantum networks, and measurement-based quantum computing. As such, a scheme for entanglement verification is necessary to ensure that a given state exhibits the requisite entangled properties. *Nonlocal games*, which consist of spatially separated players prohibited from direct communication, have the ability to indicate quantum entanglement; through measurements on a shared entangled state, the players may implement a quantum strategy that bests any classical strategy. The Clauser-Horne-Shimony-Holt (CHSH) game [CHSH69] is an example of such a nonlocal game that discriminates between classical and quantum approaches. The crux of these games lies in the correlations engendered by quantum entanglement—entangled states exhibit quantum correlations that cannot be replicated through classical statistics, a phenomenon known as Bell non-locality [Bel64]. Thus, as the measurements that players make on their shared entangled state will be non-classically correlated, the players can achieve a higher likelihood of success by basing their answers off the results of their measurements.

So, if players have access to an entangled state, then they can win the CHSH game with a higher probability than with any classical strategy. In order for the game to certify quantum entanglement, however, the converse must also be true: that is, if the correlations observed in the CHSH game surpass some classical threshold, then quantum entanglement *must* be present. Tying the observation of a *specific* set of correlations to a *specific* entangled state, such as a singlet, is known as *self-testing*. Coined by Mayers and Yao in [MY04], self-testing aims to identify particular correlations that can only be realized by particular physical states. Self-testing schemes can then be employed to achieve *device-independent* verification of specific entangled states: without any knowledge of the details of physical preparation, the presence of a particular state can be checked by simply conducting a set of correlation measurements.

This work is a brief introduction to the self-testing of quantum systems. A mathematical formulation of self-testing is first presented. As a concrete example, the CHSH game is shown to be a self-test for one singlet. Further extensions and future directions are highlighted in the conclusion. For a comprehensive review of self-testing, see [ŠB20].

2 Robust self-testing[1]

Let's say that Alice and Bob have access to a device which purports to output some bipartite entangled state $|\psi\rangle_{\mathcal{AB}}$. They then wish to check that the actual physical state $|\phi\rangle_{\mathcal{A'B'}}$ is equivalent to the target $|\psi\rangle_{\mathcal{AB}}$. Here, $\mathcal{A}$ ($\mathcal{B}$) denotes Alice's (Bob's) respective subsystem, with primes indicating the physical, rather than the ideal, subsystem. To do so, they conduct a set of measurements on their respective parts of $\rho_{\mathcal{A'B'}}$. They repeat these measurements for multiple trials, obtaining a new, identical state $|\phi\rangle_{\mathcal{A'B'}}$ from the device for each trial. In this manner, after gathering their outcomes from repeated trials, they will be able to estimate the correlation of their outcomes. If they find that this correlation reaches a certain maximal value, then they can say that the physical state $|\phi\rangle_{\mathcal{A'B'}}$ outputted by the device is, in some sense, the same as the desired entangled state $|\psi\rangle_{\mathcal{AB}}$. This process is known as the *self-testing* of $|\psi\rangle_{\mathcal{AB}}$.

Now, let's formulate this procedure more rigorously. We want to test whether a physical state $|\phi\rangle_{\mathcal{A'B'}}$[2] in $\mathcal{H}_{\mathcal{A'}} \otimes \mathcal{H}_{\mathcal{B'}}$ is the same as an ideal entangled state $|\psi\rangle_{\mathcal{AB}}$ in $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ [3]. Let Alice's (Bob's)

[1] The ideas presented here take inspiration from [ŠB20].

[2] We assume the form of a pure state WLOG as we can always consider $|\phi\rangle_{\mathcal{A'B'}P}$ to be the purification of some $\rho_{\mathcal{A'B'}}$, with the operators in the self-testing scheme acting trivially on the purification space P.

[3] Note that we make no assumptions about the physical Hilbert spaces $\mathcal{H}_{\mathcal{A'}}, \mathcal{H}_{\mathcal{B'}}$; they do not need to be the same dimension as $\mathcal{H}_{\mathcal{A}}$, $\mathcal{H}_{\mathcal{B}}$.

measurements on subsystem $\mathcal{A}'$ ($\mathcal{B}'$) be labeled by $x(y)$ and their outcomes by $a(b)$. These are realized by projective operators $\{\Pi_{a|x}\}$ on subsystem $\mathcal{A}'$ and $\{\Pi_{b|y}\}$ on subsystem $\mathcal{B}'$. A correlation $P(a,b|x,y)$ is then given by

$$P(a,b|x,y) = \langle \Pi_{a|x}\Pi_{b|y}\rangle = \mathrm{Tr}\big\{|\phi\rangle\langle\phi|_{\mathcal{A}'\mathcal{B}'}\,\Pi_{a|x}\Pi_{b|y}\big\}. \tag{1}$$

Self-testing thus strives to infer the form of $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ from observing $P(a,b|x,y)$.

We must additionally quantify what it means for $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ to be "the same" as $|\psi\rangle_{\mathcal{A}\mathcal{B}}$. Here, we note that it is impossible to determine the exact form of $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ just from $P(a,b|x,y)$ alone. To see why this is true, note that the statistics of $P(a,b|x,y)$ can be reproduced by using the rotated state $U\otimes V\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ and measurements $\{U\Pi_{a|x}U^\dagger\}$, $\{V\Pi_{b|y}V^\dagger\}$, where U and V are two unitary operators. Moreover, the measurement operators may act trivially on certain degrees of freedom within a larger system. In this case, a state $|\phi\rangle\otimes|\xi\rangle$ and operators $\{\Pi_{a|x}\otimes\mathbb{1}\}$, $\{\Pi_{b|y}\otimes\mathbb{1}\}$, where the identity acts on $|\xi\rangle$, also yields the same $P(a,b|x,y)$. To account for these unknowns, we define equivalence using *local isometries*.

Local isometry

Definition 2.1. *An isometry*

$$\Phi : \mathcal{H}_{\mathcal{A}_1} \to \mathcal{H}_{\mathcal{A}_2}$$

is a linear transformation on quantum states that preserves the inner product. It can be seen as a unitary operator that has the ability to increase the dimension of the space, so

$$\Phi\,|\psi\rangle_{\mathcal{A}_1} = U\,|\psi\rangle_{\mathcal{A}_2}\,,$$

where $\dim(\mathcal{A}_2) > \dim(\mathcal{A}_1)$ *and* U *is unitary.*
A local isometry

$$\Phi_{\mathcal{A}_1}\otimes\Phi_{\mathcal{B}_1} : \mathcal{H}_{\mathcal{A}_1}\otimes\mathcal{H}_{\mathcal{B}_1} \to \mathcal{H}_{\mathcal{A}_2}\otimes\mathcal{H}_{\mathcal{B}_2}$$

consists of local quantum operations; it is a tensor product of isometries which act locally.

We are now in a position to rigorously define self-testing.

Self-testing

Definition 2.2. *The correlations* $P(a,b|x,y)$ *self-test a well-defined quantum state* $|\psi\rangle_{\mathcal{A}\mathcal{B}}$ *if for all* $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ *compatible with* $P(a,b|x,y)$*, there exists a local isometry*

$$\Phi_{\mathcal{A}'}\otimes\Phi_{\mathcal{B}'} : \mathcal{H}_{\mathcal{A}'}\otimes\mathcal{H}_{\mathcal{B}'} \to \mathcal{H}_{\mathcal{A}\bar{\mathcal{A}}}\otimes\mathcal{H}_{\mathcal{B}\bar{\mathcal{B}}}$$

such that

$$\Phi_{\mathcal{A}'}\otimes\Phi_{\mathcal{B}'}\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'} = |\psi\rangle_{\mathcal{A}\mathcal{B}}\otimes|junk\rangle_{\bar{\mathcal{A}}\bar{\mathcal{B}}} \tag{2}$$

This means that if $P(a,b|x,y)$ are observed on some $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$, then there must exist a local channel, or isometry, through which the target state $|\psi\rangle_{\mathcal{A}\mathcal{B}}$ can be extracted, along with a leftover junk state $|junk\rangle_{\bar{\mathcal{A}}\bar{\mathcal{B}}}$. Here, we first note some important remarks regarding self-testing.

Remarks

1. The actual isometry to extract $|\psi\rangle_{\mathcal{A}\mathcal{B}}$ from $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ does not need to be performed in the laboratory; only a proof that such an isometry exists is necessary.

2. The correlations $P(a,b|x,y)$ are obtained by averaging the results of independent and identically distributed (i.i.d.) rounds of measurements $\{\Pi_{a|x}\}$, $\{\Pi_{b|y}\}$ on $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$. This means that the state $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ and the measurement operators must be identical in each trial, such that measurement outcomes follow the same distribution and do not depend on results from previous trials.

3. Though the definitions presented above refer to bipartite systems, self-testing can be straightforwardly generalized to a multipartite state by considering an isometry that acts locally on each part of the system.

Crucially, however, we will never measure the exact value of $P(a,b|x,y)$ due to the statistical limitation of a finite sample size. Moreover, because of experimental noise, we might not expect our physical state $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ to exactly satisfy Eq. 2. Thus, we must build some tolerance for error into our definition of self-testing; this is known as *robustness*.

To do so, we use the vector norm $||\cdot||$ as a measure of distance,

$$||\,|\psi\rangle\,|| = \sqrt{|\,\langle\psi|\psi\rangle\,|^2}.$$

Robustness can then be incorporated into our definition of self-testing as follows:

Robust self-testing

Definition 2.3. *The correlations $P'(a,b|x,y)$ self-test $|\psi\rangle_{\mathcal{A}\mathcal{B}}$ with error δ if for any $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ compatible with $P'(a,b|x,y)$, there exists a local isometry $\Phi_{\mathcal{A}'}\otimes\Phi_{\mathcal{B}'}$ such that*

$$||\Phi_{\mathcal{A}'}\otimes\Phi_{\mathcal{B}'}\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'} - |\psi\rangle_{\mathcal{A}\mathcal{B}}\otimes|junk\rangle_{\bar{\mathcal{A}}\bar{\mathcal{B}}}\,|| \leq \delta$$

for some state $|junk\rangle_{\bar{\mathcal{A}}\bar{\mathcal{B}}}$.

Now that we know the formal definition of a self-test, we may wonder what types of measurements $\{\Pi_{a|x}\}$, $\{\Pi_{b|y}\}$ give rise to correlations $P(a,b|x,y)$ that actually have the ability to self-test a specific state $|\psi\rangle_{\mathcal{A}\mathcal{B}}$. In what follows, we introduce the CHSH game, a non-local game that can be employed to robustly self-test for one singlet.

3 CHSH game

3.1 Introduction

In the CHSH game, Alice and Bob each receive a uniformly chosen bit x, y from the referee, $x,y \sim \text{Unif}(\{0,1\})$. Alice and Bob then reply to the referee with bits a, $b \in \{0,1\}$. They win the game if

$$x \wedge y = a \oplus b \tag{3}$$

Here $\oplus$ indicates addition modulo 2 or XOR, while $\wedge$ is a logical AND. Now, any classical strategy has a maximal success probability of $\frac{3}{4}$. A proof of this is given in [Mer17], and a general overview of how this limit appears is given in Appendix A.

In the quantum case, Alice and Bob can share some entangled state $|\psi\rangle_{\mathcal{A}\mathcal{B}}$. Depending on the bit x Alice receives, she then performs the measurement $\Pi_{a|x}$ with result a. Similarly, Bob performs $\Pi_{b|y}$. Then, the probability of winning is given by

$$P_{win} = \frac{1}{4}\sum_{\{a,b,x,y|x\wedge y=a\oplus b\}} \langle\psi|_{\mathcal{A}\mathcal{B}}\,\Pi_{a|x}\otimes\Pi_{b|y}\,|\psi\rangle_{\mathcal{A}\mathcal{B}}$$

Note that this expression also holds classically with the redefinition

$$\langle\psi|_{\mathcal{AB}}\,\Pi_{a|x}\otimes\Pi_{b|y}\,|\psi\rangle_{\mathcal{AB}}=\langle\Pi_{a|x}\otimes\Pi_{b|y}\rangle\to p(a,b|x,y),$$

where $p(a,b|x,y)$ is the probability of returning a,b given inputs x,y.

We can explore this in even greater detail. If the input bits (x,y) are either $(0,1)$, $(1,0)$, or $(0,0)$, then the probability of winning minus the probability of losing is

$$\langle\Pi_{0|x}\otimes\Pi_{0|y}\rangle+\langle\Pi_{1|x}\otimes\Pi_{1|y}\rangle-\langle\Pi_{0|x}\otimes\Pi_{1|y}\rangle-\langle\Pi_{1|x}\otimes\Pi_{0|y}\rangle=\langle(\Pi_{0|x}-\Pi_{1|x})\otimes(\Pi_{0|y}-\Pi_{1|y})\rangle.$$

Similarly, if the input bits (x,y) are $(1,1)$, then the probability of winning minus the probability of losing becomes $-\langle(\Pi_{0|x}-\Pi_{1|x})\otimes(\Pi_{0|y}-\Pi_{1|y})\rangle$. Thus, defining

$$A_x=\Pi_{0|x}-\Pi_{1|x},\quad B_y=\Pi_{0|y}-\Pi_{1|y}\tag{4}$$

we see that overall, $P_{win}-P_{lose}=\frac{1}{4}\Big(\langle A_0B_0\rangle+\langle A_1B_0\rangle+\langle A_0B_1\rangle-\langle A_1B_1\rangle\Big)$ where

$$\begin{aligned}\langle A_xB_y\rangle&=\langle\psi|_{\mathcal{AB}}\,A_xB_y\,|\psi\rangle_{\mathcal{AB}}\ \text{(quantum case)}\\&=\sum_{a,b\in\{0,1\}}(-1)^{a\oplus b}p(a,b|x,y)\ \text{(classical case)}.\end{aligned}$$

So, as $P_{win}\le\frac{3}{4}$ ($P_{win}-P_{lose}\le\frac{1}{2}$) classically, then the following inequality must hold for *any classical correlations*:

CHSH Inequality

$$\langle A_0B_0\rangle+\langle A_1B_0\rangle+\langle A_0B_1\rangle-\langle A_1B_1\rangle\le 2\tag{5}$$

Known as the *CHSH inequality*, Eq. 5 was first derived by Clauser, Horne, Shimony, and Holt in [CHSH69].

Now, it turns out that if Alice and Bob share a maximally entangled state of two qubits

$$|\psi\rangle_{\mathcal{AB}}=|\phi^+\rangle_{\mathcal{AB}}=\frac{|00\rangle_{\mathcal{AB}}+|11\rangle_{\mathcal{AB}}}{\sqrt{2}},$$

which we refer to from now on as a *singlet*, and conduct the measurements

$$A_0=\mathbf{X}^A\quad A_1=\mathbf{Z}^A\quad B_0=\frac{\mathbf{X}^B+\mathbf{Z}^B}{\sqrt{2}}\quad B_1=\frac{\mathbf{X}^B-\mathbf{Z}^B}{\sqrt{2}}$$

where $\mathbf{X},\mathbf{Z}$ are Pauli operators, then they can achieve $P_{win}=\cos(\pi/8)^2\approx 0.85$. This is the maximum success probability for a quantum strategy, thus maximally violating the CHSH inequality (Eq. 5) with value CHSH $=2\sqrt{2}>2$. We now show that observing a maximal violation of CHSH $=2\sqrt{2}$, with some tolerance for error, actually self-tests for the singlet state $|\phi^+\rangle_{\mathcal{AB}}=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

3.2 Robust self-testing of one singlet

Here, we follow the argument presented in [MYS12] to show that the CHSH game with maximal success probability (violating Eq. 5 with CHSH $=2\sqrt{2}$) robustly self-tests for a singlet $|\phi^+\rangle$. The ideal case was proven in [MY04].

First, we will present Ref. [MYS12]'s main theorem. Then, we will go over a sketch of the proof and make some remarks about their result. Here, a subscript $\mathcal{A}$ ($\mathcal{B}$) will denote Alice's (Bob's) subsystem, with primes indicating physical subsystems. Primed operators indicate physical observables, while unprimed $\mathbf{X}, \mathbf{Z}$ refer to Pauli operators. For example, due to noise and extra experimental degrees of freedom, a physical $\mathbf{X}'$ may not implement a perfect Pauli $\mathbf{X}$. We wish to self-test a physical state $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ as a singlet $|\phi^+\rangle_{\mathcal{A}\mathcal{B}} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

CHSH bound is a robust self-test of the singlet

Theorem 3.1. *Suppose that the observables A'_0, A'_1, B'_0 and B'_1 with eigenvalues ± 1 act on a state $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ such that*

$$\langle\phi| \left(A'_0 B'_0 + A'_1 B'_0 + A'_0 B'_1 - A'_1 B'_1 \right) |\phi\rangle \geq 2\sqrt{2} - \epsilon \tag{6}$$

Then, there exists local observables $\{\mathbf{X}'_{\mathcal{A}'}, \mathbf{Z}'_{\mathcal{A}'}\}$ (functions of A'_i) and $\{\mathbf{X}'_{\mathcal{B}'}, \mathbf{Z}'_{\mathcal{B}'}\}$ (functions of B'_i) with eigenvalues ± 1 and a local isometry $\Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}$ such that

$$||\Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}(\mathbf{M}'_{\mathcal{A}'}\mathbf{N}'_{\mathcal{B}'} |\phi\rangle) - (\mathbf{M}_{\mathcal{A}}\mathbf{N}_{\mathcal{B}} |\phi^+\rangle_{\mathcal{A}\mathcal{B}}) \otimes |junk\rangle|| \leq \delta \tag{7}$$

for $\mathbf{M}, \mathbf{N} \in \{\mathbb{1}, \mathbf{X}, \mathbf{Z}\}$ where $\delta = O(\sqrt{\epsilon})$.

Proof Sketch To prove Eq. 7 from Eq. 6, we can first explicitly construct $\{\mathbf{X}'_{\mathcal{A}'}, \mathbf{Z}'_{\mathcal{A}'}\}$ and $\{\mathbf{X}'_{\mathcal{B}'}, \mathbf{Z}'_{\mathcal{B}'}\}$ from A'_0, A'_1, B'_0 and B'_1. This is done by defining

$$\mathbf{X}'_{\mathcal{A}'} = A'_0 \;\; \mathbf{Z}'_{\mathcal{A}'} = A'_1 \;\; \mathbf{X}'_{\mathcal{B}'} = \frac{B'_0 + B'_1}{|B'_0 + B'_1|} \;\; \mathbf{Z}'_{\mathcal{B}'} = \frac{B'_0 - B'_1}{|B'_0 - B'_1|}. \tag{8}$$

Here, $|M| = \sqrt{M^2}$, where zero eigenvalues of M are taken to be 1 in $M/|M|$. Then, the following bounds can be shown using Eq. 6 along with the Cauchy-Schwartz and triangle inequalities,

$$\begin{aligned} &||(\mathbf{X}'_{\mathcal{A}'}\mathbf{Z}'_{\mathcal{A}'} + \mathbf{Z}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{A}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'}|| \leq \epsilon_1, \;\; ||(\mathbf{X}'_{\mathcal{B}'}\mathbf{Z}'_{\mathcal{B}'} + \mathbf{Z}'_{\mathcal{B}'}\mathbf{X}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'}|| \leq \epsilon_1 \\ &||(\mathbf{X}'_{\mathcal{A}'} - \mathbf{X}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'}|| \leq \epsilon_2, \;\; ||(\mathbf{Z}'_{\mathcal{A}'} - \mathbf{Z}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'}|| \leq \epsilon_2, \end{aligned} \tag{9}$$

where $\epsilon_1 = \mathrm{O}(\sqrt{\epsilon})$ and $\epsilon_2 = \mathrm{O}(\epsilon^{1/4})$. Moreover, the explicit form of the isometry $\Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}$ can be constructed as in Fig. 1. Note that this takes the form of a partial swap gate, which swaps the physical state $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ onto two ancilla qubits. To analyze this isometry, we can consider when $\mathbf{M} = \mathbf{N} = \mathbb{1}$. Then, we have

$$\begin{aligned} \Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}(|\phi\rangle_{\mathcal{A}'\mathcal{B}'}) = \frac{1}{4}\Big[&(1 + \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'}) |00\rangle_{\mathcal{A}\mathcal{B}} + \mathbf{X}'_{\mathcal{B}'}(1 + \mathbf{Z}'_{\mathcal{A}'})(1 - \mathbf{Z}'_{\mathcal{B}'}) |01\rangle_{\mathcal{A}\mathcal{B}} \\ &+ \mathbf{X}'_{\mathcal{A}'}(1 - \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'}) |10\rangle_{\mathcal{A}\mathcal{B}} + \mathbf{X}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{B}'}(1 - \mathbf{Z}'_{\mathcal{A}'})(1 - \mathbf{Z}'_{\mathcal{B}'}) |11\rangle_{\mathcal{A}\mathcal{B}}\Big] |\phi\rangle_{\mathcal{A}'\mathcal{B}'}. \end{aligned} \tag{10}$$

Let's look at the ideal case, in which $\epsilon_1, \epsilon_2 = 0$ in Eq. 9. Then, $\mathbf{Z}'_{\mathcal{A}'} |\phi\rangle_{\mathcal{A}'\mathcal{B}'} = \mathbf{Z}'_{\mathcal{B}'} |\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ and $\mathbf{X}'_{\mathcal{A}'} |\phi\rangle_{\mathcal{A}'\mathcal{B}'} = \mathbf{X}'_{\mathcal{B}'} |\phi\rangle_{\mathcal{A}'\mathcal{B}'}$. So, $(1 \pm \mathbf{Z}'_{\mathcal{A}'})(1 \mp \mathbf{Z}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'} = 0$, and the coefficients of $|01\rangle_{\mathcal{A}\mathcal{B}}$ and $|10\rangle_{\mathcal{A}\mathcal{B}}$ go to zero in Eq. 10. Finally, the term in front of $|11\rangle_{\mathcal{A}\mathcal{B}}$ can be simplified to

$$\begin{aligned} \mathbf{X}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{B}'}(1 - \mathbf{Z}'_{\mathcal{A}'})(1 - \mathbf{Z}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'} &= (1 + \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'})\mathbf{X}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{B}'} |\phi\rangle_{\mathcal{A}'\mathcal{B}'} \\ &= (1 + \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'}) |\phi\rangle_{\mathcal{A}'\mathcal{B}'} \end{aligned}$$

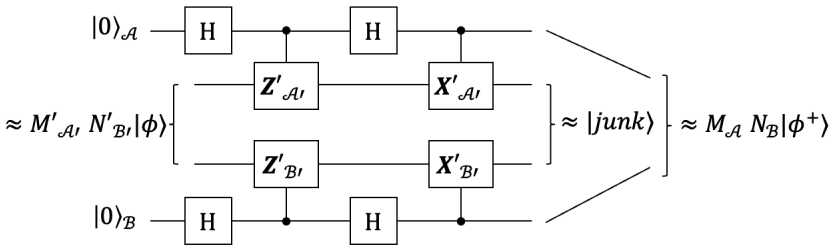

Figure 1: Local isometry $\Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}$, where $\mathbf{M}, \mathbf{N} \in \{\mathbb{1}, \mathbf{X}, \mathbf{Z}\}$.

where we have used the ideal anticommutation relations from Eq. 9, as well as $\mathbf{X}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{B}'}\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'} = \mathbf{X}'^2_{\mathcal{A}'}\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'} = |\phi\rangle_{\mathcal{A}'\mathcal{B}'}$. From here, we can see that Eq. 10 becomes

$$\Phi_{\mathcal{A}} \otimes \Phi_{\mathcal{B}}(|\phi\rangle_{\mathcal{A}'\mathcal{B}'}) = \frac{|00\rangle_{\mathcal{A}\mathcal{B}} + |11\rangle_{\mathcal{A}\mathcal{B}}}{\sqrt{2}} \otimes \frac{1}{2\sqrt{2}}(1 + \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'})\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$$

where we can identify $\frac{1}{2\sqrt{2}}(1 + \mathbf{Z}'_{\mathcal{A}'})(1 + \mathbf{Z}'_{\mathcal{B}'})\,|\phi\rangle_{\mathcal{A}'\mathcal{B}'} \equiv |junk\rangle$. This explicitly verifies that in the ideal case, the isometry constructed in Fig. 1 perfectly takes our physical state $|\phi\rangle$ to the singlet $|\phi^+\rangle$, up to some extra junk state.

Finally, the error $\delta \sim \epsilon_1 + \epsilon_2 = O(\sqrt{\epsilon})$ in Eq. 7 can be derived using the action of this specific isometry and the bounds in Eq. 9; this derivation invokes the triangle inequality and the unitarity and Hermiticity of the operators. □

Remarks

1. A crucial part of this result (Eq. 9) relies on the fact that Alice and Bob each measure anti-commuting operators: $\mathbf{X}'_{\mathcal{A}'}\mathbf{Z}'_{\mathcal{A}'} + \mathbf{Z}'_{\mathcal{A}'}\mathbf{X}'_{\mathcal{A}'} \approx 0$, $\mathbf{X}'_{\mathcal{B}'}\mathbf{Z}'_{\mathcal{B}'} + \mathbf{Z}'_{\mathcal{B}'}\mathbf{X}'_{\mathcal{B}'} \approx 0$. Indeed, as Pauli operators anti-commute, we see that this holds in the example where they measure ideal Pauli operators.

2. In Eq. 7, for $\mathbf{M}, \mathbf{N} = \mathbb{1}$, we explicitly see that the isometry takes $|\phi\rangle_{\mathcal{A}'\mathcal{B}'}$ into $|\phi^+\rangle_{\mathcal{A}\mathcal{B}} \otimes |junk\rangle$. However, as Eq. 7 also holds for Pauli $\mathbf{M}, \mathbf{N}$, this bound implies that any measurements which almost maximally violate the CHSH inequality must also approximate Pauli matrices. This result—that any approximately optimal stategy must have the same structure as an ideal strategy—is known as *rigidity*.

4 Conclusion

Here, we have given a concise introduction into the self-testing of entangled states, giving the CHSH game as an example of a robust self-test for a singlet state. Other non-local games, such as the Mermin-Peres magic square [Mer90] [Per90], have also been shown to have the capacity to self-test certain quantum states. For example, [WBMS16] showed that the magic square game could robustly self-test for two singlets. Moreover, self-tests for multiple entangled pairs can also be constructed by repeating the CHSH or magic square games multiple times—either in series over multiple rounds, or in parallel in one round. For instance, [RUV13] showed that a serially repeated CHSH game was rigid, while [CN16] proved the rigidity of a parallel-repeated magic square game.

Open directions of research include the development of self-testing strategies for d dimensional systems that do not simply extend from lower-dimensional cases, as touched upon in [SAT+17], as well as the exploration of self-testing for non- i.i.d. rounds of measurement, as examined by [BRS+21].

References

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[BRS+21] Jean-Daniel Bancal, Kai Redeker, Pavel Sekatski, Wenjamin Rosenfeld, and Nicolas Sangouard. Self-testing with finite statistics enabling the certification of a quantum network link. *Quantum*, 5:401, mar 2021.

[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.

[CN16] Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid, 2016.

[Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990.

[Mer17] Logan Meredith. The CHSH game as a Bell test thought experiment. 2017.

[MY04] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, jul 2004.

[MYS12] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, oct 2012.

[Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3):107–108, 1990.

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, 4 2013.

[SAT+17] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, Jul 2017.

[ŠB20] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020.

[WBMS16] Xingyao Wu, Jean Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93, 6 2016.

A Classical CHSH

Suppose Alice and Bob send back a_x, b_y, dependent on the bits x, y that they receive. The possiblities for x, y and a_x, b_y are listed in Table 1.

x	y	$x \wedge y$	$=a_x \oplus b_y$
0	0	0	$= a_0 \oplus b_0$
0	1	0	$= a_0 \oplus b_1$
1	0	0	$= a_1 \oplus b_0$
1	1	1	$= a_1 \oplus b_1$
	$\oplus$	$= 1$	$= 0$

Table 1: Possible combinations of a_x, b_y for given x, y in the CHSH game.

Because $\oplus$ is commutative and $\forall\ c \in \{0, 1\}$, $c \oplus c = 0$, the fourth column of Table 1 must add to 0 modulo 2. However, the third column adds to 1 modulo 2. Thus, it is impossible for any strategy of a_x, b_y to satisfy all four relations in Table 1 at once: a win cannot be guaranteed. However, three out of the four can be satisfied simply by choosing $a_x, b_y = 0$ for all x, y, for example, leading to a success rate of $\frac{3}{4}$. This turns out to be the maximum success probability for any classical strategy.