Robust self-testing of partially entangled quantum systems using tilted CHSH inequalities

Cédric Bamps, Stefano Pironio

Université Libre de Bruxelles

May 15 2014

Plan

Self-testing the singlet

Qubit states at the CHSH Tsirelson bound $\mathrm{CHSH}^{\max} = 2\sqrt{2}$ are always singlets: $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ in a suitable basis.

McKague, Yang and Scarani: device independent, robust version of this: any quantum black box with $\mathrm{CHSH} = 2\sqrt{2} - \epsilon$ is equivalent to a singlet up to a local isometry $\Phi = \Phi_{\mathrm{A}} \otimes \Phi_{\mathrm{B}}$.

Using the physical measurement operators, define the unitary gates

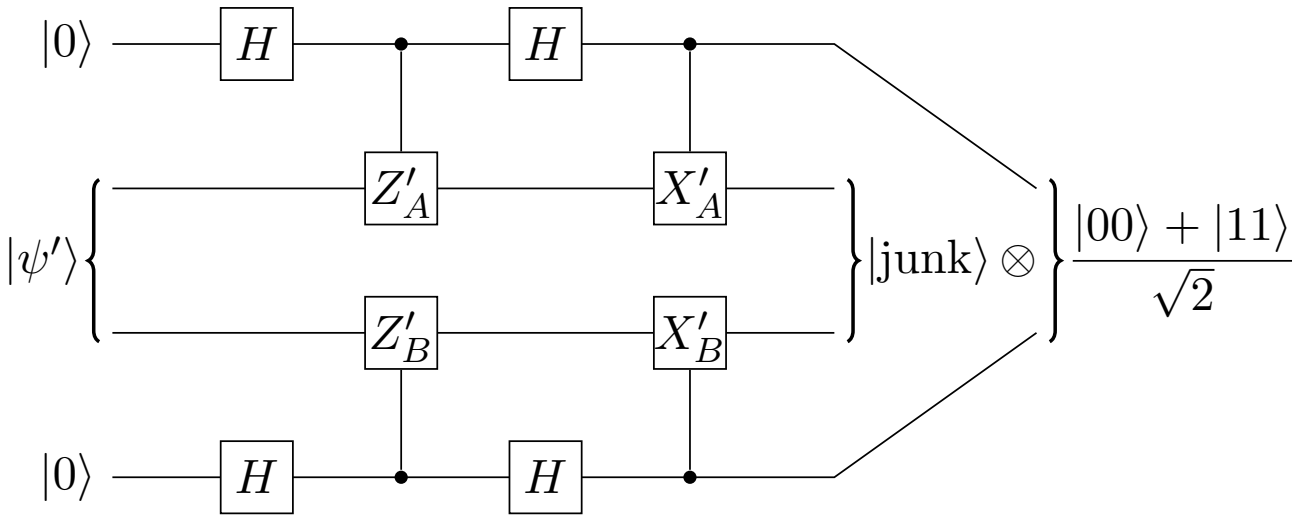
$$Z'_{\mathrm{A}} = A_0 \qquad X'_{\mathrm{A}} = A_1$$

$$Z'_{\mathrm{B}} = \frac{B_0 + B_1}{\sqrt{2}} \left| \frac{B_0 + B_1}{\sqrt{2}} \right|^{-1} \qquad X'_{\mathrm{B}} = \frac{B_0 - B_1}{\sqrt{2}} \left| \frac{B_0 - B_1}{\sqrt{2}} \right|^{-1}$$

M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012)

Self-testing the singlet

Idea: If $\mathrm{CHSH} = 2\sqrt{2}$, the measurement operators are constrained (e.g. anticommutation), and identities on the X' and Z' make this local isometry extract the singlet from the black box state $|\psi'\rangle$:



Note that $|\mathrm{junk}\rangle$ is uncorrelated to the singlet.
Robustness: for $\mathrm{CHSH} = 2\sqrt{2} - \epsilon$

$$\left\| \Phi(|\psi'\rangle) - |\mathrm{junk}\rangle\,|\phi_+\rangle \right\| \leq \mathcal{O}(\epsilon^{1/4})$$

M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012)

Tilted CHSH

Class of Bell inequalities for $0 \leq \alpha < 2$

$$I_\alpha = \alpha A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1$$

Classical bound: $\langle I_\alpha \rangle \leq \alpha + 2$
Quantum bound: $\langle I_\alpha \rangle \leq \sqrt{8 + 2\alpha^2}$

In qubits, the quantum bound is uniquely (up to a change of basis) achieved by the partially entangled state

$$|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle \qquad (0<\theta\leq\pi/4)$$

with $\tan(2\theta) = \sqrt{2\alpha^{-2} - 1/2}$ and operators

$$A_0 = Z_\mathrm{A} \qquad A_1 = X_\mathrm{A}$$
$$B_0 = \cos\mu\, Z_\mathrm{B} + \sin\mu\, X_\mathrm{B} \qquad B_1 = \cos\mu\, Z_\mathrm{B} - \sin\mu\, X_\mathrm{B}$$

with $\tan\mu = \sin(2\theta)$.

A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **10**, 100402 (2012)

Partially entangled qubits

Yang and Navascués adapted the framework to partially entangled states, using tilted CHSH violation.

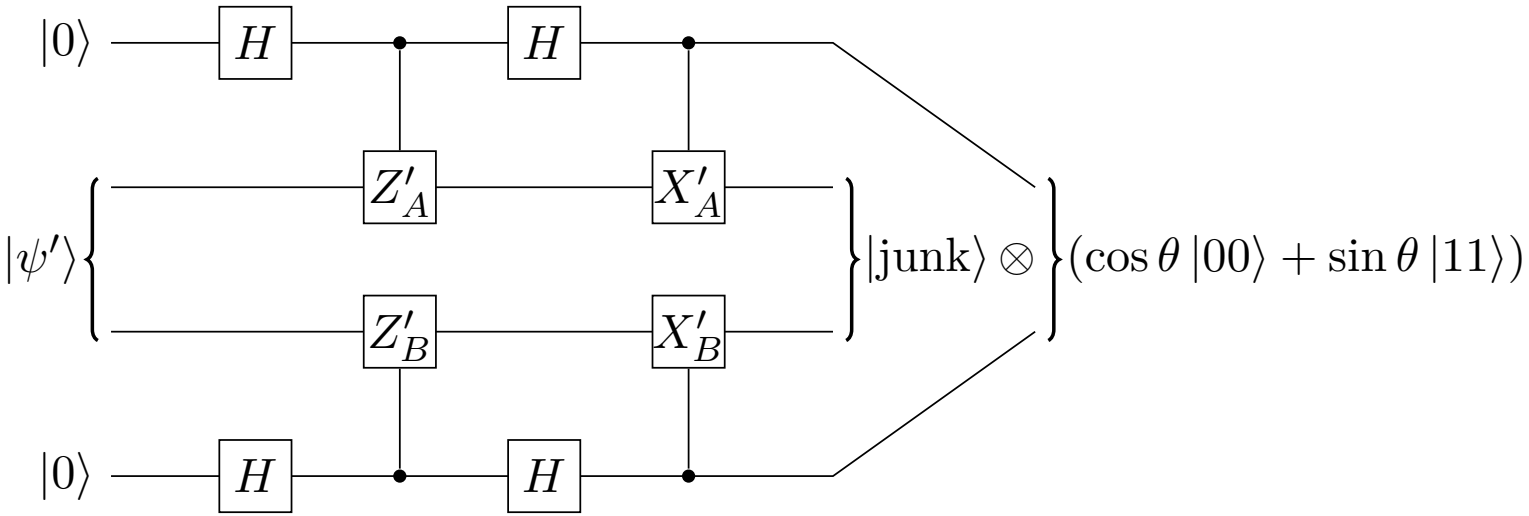
Same as above: maximal violation puts robust algebraic constraints on the measurements, that enable us to build a similar isometry to extract partial entanglement.

Again, the gates are unitarized versions of

$$Z'_{\mathrm{A}} = A_0 \qquad X'_{\mathrm{A}} = A_1$$
$$Z'_{\mathrm{B}} = (B_0 + B_1)/(2\cos\mu) \qquad X'_{\mathrm{B}} = (B_0 - B_1)/(2\sin\mu)$$

T. H. Yang and M. Navascués, Phys. Rev. A **5**, 050102 (2013)

Isometry



The isometry works under the following two conditions:

$$\left(Z'_{\mathrm{A}} - Z'_{\mathrm{B}}\right)|\psi'\rangle = 0\,,$$
$$\left(\sin\theta X'_{\mathrm{A}}\left(I + Z'_{\mathrm{B}}\right) - \cos\theta X'_{\mathrm{B}}\left(I - Z'_{\mathrm{A}}\right)\right)|\psi'\rangle = 0\,.$$

(In the ideal example of partially entangled qubits, this is easily verified.)

Operator identities

To prove these identities, Yang and Navascués use the concept of sum of squares (SOS) decomposition:

Since $\langle I_\alpha \rangle \leq I_\alpha^{\max}$ for all states,

$$\overline{\mathcal{B}}(\alpha) = I_\alpha^{\max} - I_\alpha \succeq 0\,.$$

A SOS decomposition for such a positive operator would have the form

$$I_\alpha^{\max} - I_\alpha = \overline{\mathcal{B}}(\alpha) = \sum_j P_j^\dagger(\alpha) P_j(\alpha)\,.$$

Then, if $\langle \overline{\mathcal{B}}(\alpha) \rangle = 0$ for $|\psi'\rangle$, then $\langle P_j^\dagger P_j \rangle = \| P_j |\psi'\rangle \|^2 = 0 \quad \forall j$
$\rightarrow$ one vanishing operator for $|\psi'\rangle$ for each term of the SOS!

Sum of squares for tilted CHSH

Yang and Navascués provide a SOS of five terms for $\overline{\mathcal{B}}(\alpha)$. From linear combinations of the five identities $P_j \left|\psi'\right\rangle = 0$ that follow, they deduce

$$\left(Z'_{\mathrm{A}} - Z'_{\mathrm{B}}\right) \left|\psi'\right\rangle = 0\,,$$
$$\left(\sin\theta X'_{\mathrm{A}} \left(I + Z'_{\mathrm{B}}\right) - \cos\theta X'_{\mathrm{B}} \left(I - Z'_{\mathrm{A}}\right)\right) \left|\psi'\right\rangle = 0\,.$$

which are the two identities needed for the isometry to work.

Problem: due to an unnoticed linear dependency in their P_j, the second identity is not recovered from their SOS.

Can we use the same SOS approach to complete their proof?

SOS search formulated as SDP

Start from any set of operators $\{R_j\}$ from which we expect to build the operators $P_j = \sum_{k=1}^{m} N_{jk} R_k$ of a SOS decomposition of $\overline{\mathcal{B}}$.

$$\overline{\mathcal{B}} = \sum_{j=1}^{n} P_j^\dagger P_j = \begin{pmatrix} R_1^\dagger \\ \vdots \\ R_m^\dagger \end{pmatrix} \cdot M \cdot \begin{pmatrix} R_1 & \dots & R_m \end{pmatrix}$$

with $M = N^\dagger \cdot N \succeq 0 \Rightarrow$ positivity constraint on M.
The equality above puts linear constraints on M.

Any $M \succeq 0$ satisfying those constraints will give us a SOS decomposition for $\overline{\mathcal{B}}$. This is exactly the kind of constraints that we find in semidefinite programming! From here, we could explore the problem numerically.

Simplifying the search: Elimination

To keep things simple, we look for SOS terms in the space spanned by the basis of nine operators

$$\mathcal{S}_{1+AB} = \{I, A_0, A_1\} \otimes \{I, B_0, B_1\}$$

Not all combinations are good candidates for P_j.
All candidates for P_j should work when the black box state $|\psi'\rangle$ and operators are the ideal maximally violating qubit system.

$\rightarrow$ We try all possible identities $R_j |\psi'\rangle = 0$ in this ideal setting, and find a basis of linearly independent R_j. For example, $R_1 = Z'_{\mathrm{A}} - Z'_{\mathrm{B}}$ and $R_2 = I - Z'_{\mathrm{A}} Z'_{\mathrm{B}}$ are seen to vanish in the ideal setting, where $|\psi'\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ and $Z' = Z$.

Simplifying the search: Candidates

The basis for the candidate subspace of $\mathcal{S}_{1+AB}$ is the following:

$$R'_1 = Z'_{\mathrm{A}} - Z'_{\mathrm{B}} \tag{1}$$
$$R'_2 = I - Z'_{\mathrm{A}} Z'_{\mathrm{B}} \tag{2}$$
$$R'_3 = cX'_{\mathrm{A}} - sZ'_{\mathrm{A}} X'_{\mathrm{B}} - X'_{\mathrm{A}} Z'_{\mathrm{B}} \tag{3}$$
$$R'_4 = cX'_{\mathrm{B}} - sX'_{\mathrm{A}} Z'_{\mathrm{B}} - Z'_{\mathrm{A}} X'_{\mathrm{B}} \tag{4}$$
$$R'_5 = sX'_{\mathrm{A}} X'_{\mathrm{B}} - Z'_{\mathrm{A}} Z'_{\mathrm{B}} + cZ'_{\mathrm{A}} \tag{5}$$

with $c = \cos(2\theta)$ and $s = \sin(2\theta)$.

SOS operators P_j in $\mathcal{S}_{1+AB}$ will be in this subspace.

Simplifying the search: Symmetry

We are now left with the problem of finding a 5×5 positive semidefinite matrix satisfying linear constraints. A symmetry in the Bell operator I_α allows us to further simplify the problem:

Recall that $I_\alpha = \alpha A_0 + A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1$.
This is symmetric under $A_1 \to -A_1$, $B_0 \leftrightarrow B_1$.
$\to$ Applying this symmetry to an SOS M_1 can give a new SOS M_2.

The convex combination $(M_1 + M_2)/2$ is yet another SOS, this time with a block structure if the basis $\{R_j\}$ is chosen well.

Simplifying the search: Symmetry

More precisely, we can choose the basis $\{R_j\}$ such that some R_j are invariant under the symmetry transformation of I_α while the others change sign.
We are effectively separating the irreducible components of the representation space $\mathrm{span}(\{R_j\})$ of the finite cyclic group $\mathcal{C}_2$.

We find three R_j in the parity representation and two in the identity representation.

This limits our search to $M \succeq 0$ with a $3 \oplus 2$ block-diagonal structure!

SOS of I_α in $\mathcal{S}_{1+AB}$ for $\theta = \pi/8$

We want a class of general SOS to self-test for all θ. Let's try $\pi/8$ to get an insight.
Imposing the linear constraints on M, we find

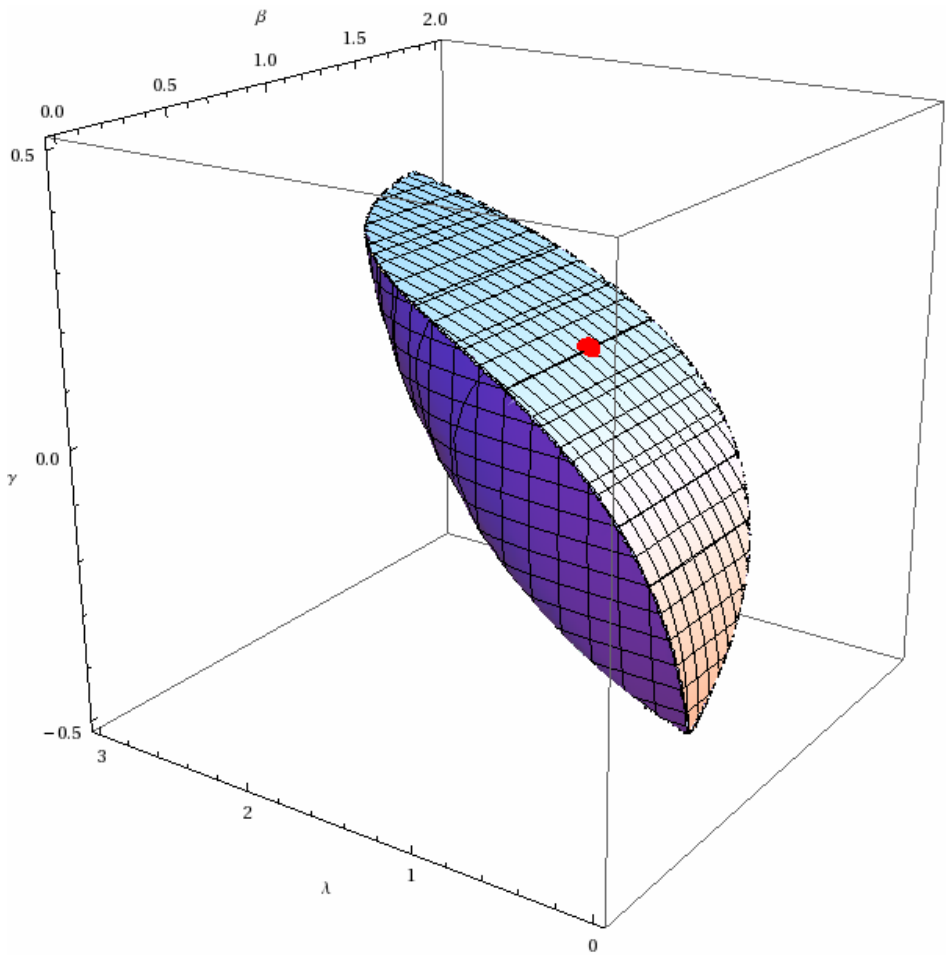
$$8\sqrt{\frac{2}{3}}M = \begin{pmatrix} \beta & \frac{-1}{\sqrt{2}} & \frac{3\gamma}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{5}{3} - \beta + \frac{\gamma}{2} & \frac{1}{3} - 2\gamma \\ \frac{3\gamma}{\sqrt{2}} & \frac{1}{3} - 2\gamma & 2 + 3\gamma - \lambda \end{pmatrix} \oplus \begin{pmatrix} \frac{2}{3} - \gamma & \frac{-\sqrt{2}}{3} - \sqrt{2}\gamma \\ \frac{-\sqrt{2}}{3} - \sqrt{2}\gamma & \lambda \end{pmatrix}$$

$\rightarrow$ three real degrees of freedom left.

We now need to impose $M \succeq 0$.

SOS of I_α in $\mathcal{S}_{1+AB}$ for $\theta = \pi/8$

Semidefinite positive subset visualized:



Corners of the set

Two extremal points stand out in this solution set. On those "corners", each of the two blocks of M is of rank 1. Therefore we easily find a minimal square root N such that $N^\dagger N = M$.

$\rightarrow$ This gives us two SOS decompositions for $I_{\alpha(\pi/8)}$. Moreover, their generalization for all θ is easily guessed!

General SOS decompositions for I_α

Result:

Two SOS for I_α

$$\begin{aligned}\overline{\mathcal{B}}(\alpha) &= \frac{1}{2I_\alpha^{\max}}\left[\overline{\mathcal{B}}^2 + \left(\alpha A_1 - \mathrm{CHSH}'\right)^2\right] \\ &= \frac{1}{2I_\alpha^{\max}}\left[\left(2A_0 - I_\alpha^{\max}\frac{B_0+B_1}{2} + \frac{\alpha}{2}\mathrm{CHSH}''\right)^2\right. \\ &\qquad \left. + \left(2A_1 - I_\alpha^{\max}\frac{B_0-B_1}{2} + \frac{\alpha}{2}\mathrm{CHSH}'''\right)^2\right]\end{aligned}$$

where CHSH', CHSH'' and CHSH''' are some permutations of the CHSH operator.

Vanishing operators

Two SOS of two terms each $\rightarrow$ four independent S_j such that $S_j |\psi'\rangle = 0$. We expected at most five. We find the fifth one by left-multiplication by A_0 of a specific combination of the known S_j. The identities needed by the self-testing isometry follow automatically.

$\rightarrow$ We have completed the proof for the claims of Yang and Navascués' paper. The same SOS methods are used, so their proof of robustness stands.

Self-testing X' and Z'

The isometry maps a maximally violating state to the corresponding partially entangled qubit state. Is it the same for the measurement operators? Equivalently, do we find that

$$\langle\psi'|\, M'_{\mathrm{A}} N'_{\mathrm{B}}\, |\psi'\rangle \simeq \langle\psi|\, M_{\mathrm{A}} N_{\mathrm{B}}\, |\psi\rangle \qquad (M, N \in \{I, X, Z\})?$$

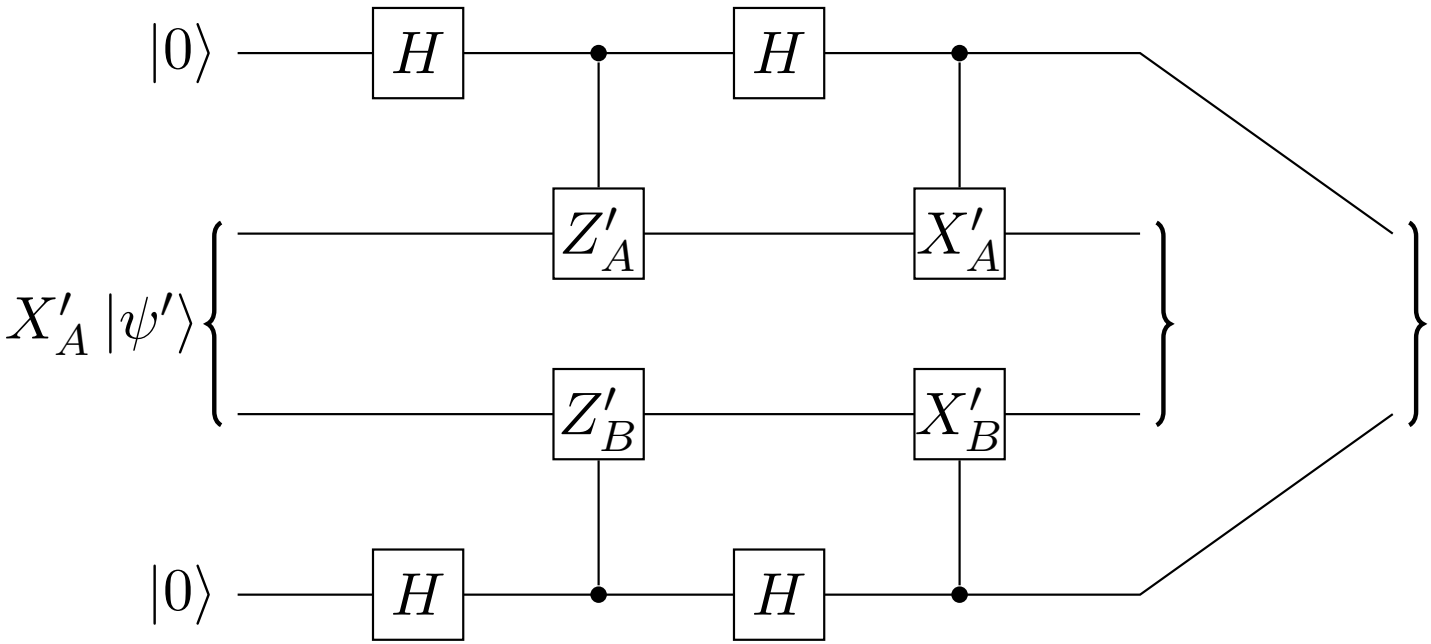
One extra ingredient is needed: this anticommutation relation for both parties:

$$\{X'_{\mathrm{A}}, Z'_{\mathrm{A}}\}\, |\psi'\rangle = \{X'_{\mathrm{B}}, Z'_{\mathrm{B}}\}\, |\psi'\rangle = 0$$

Alice's side: follows from the five identities proved earlier.
Bob's side: true by definition.

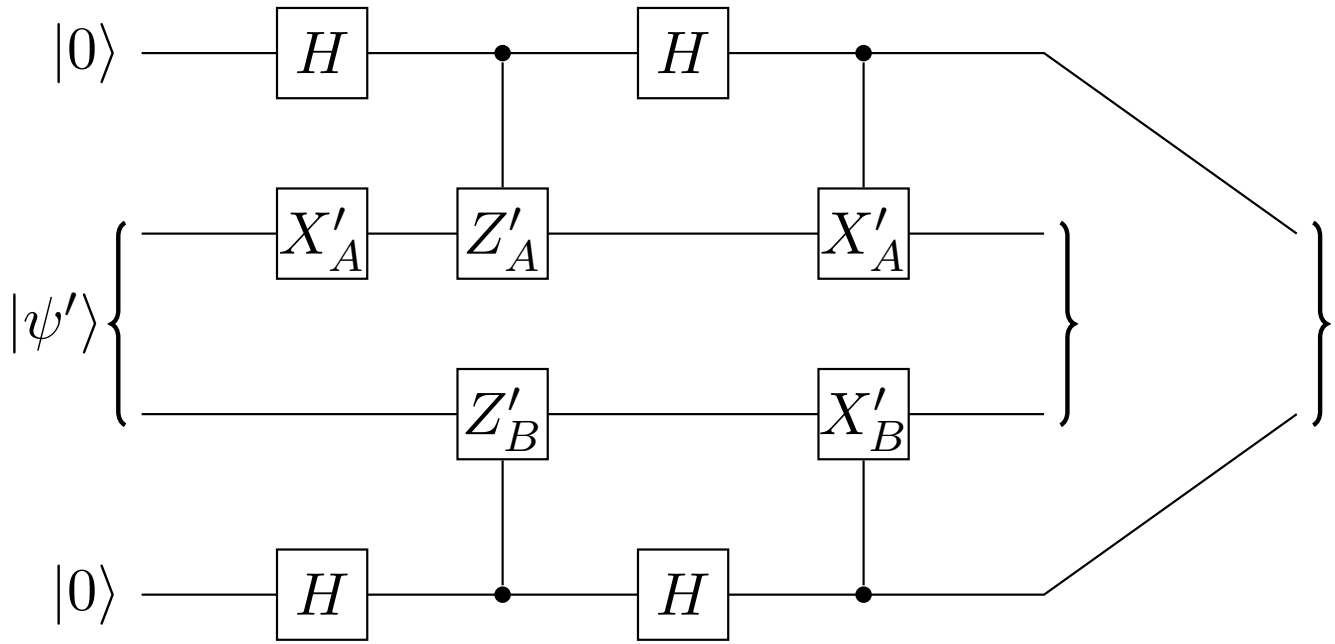
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



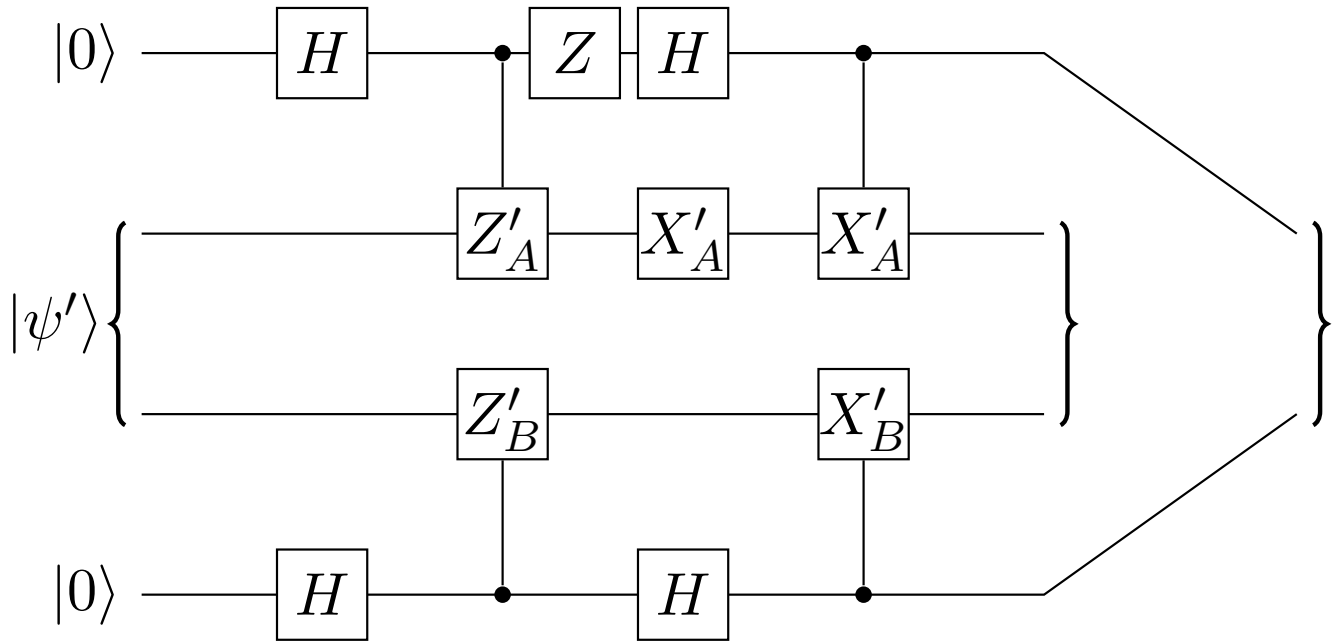
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



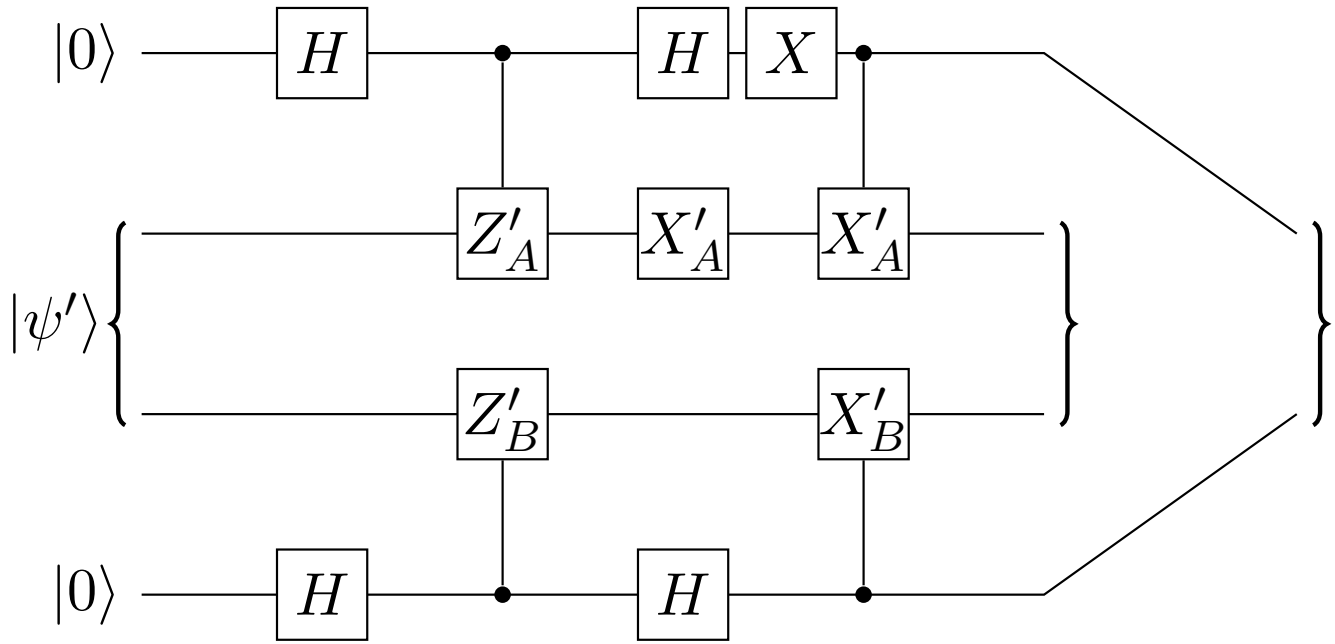
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



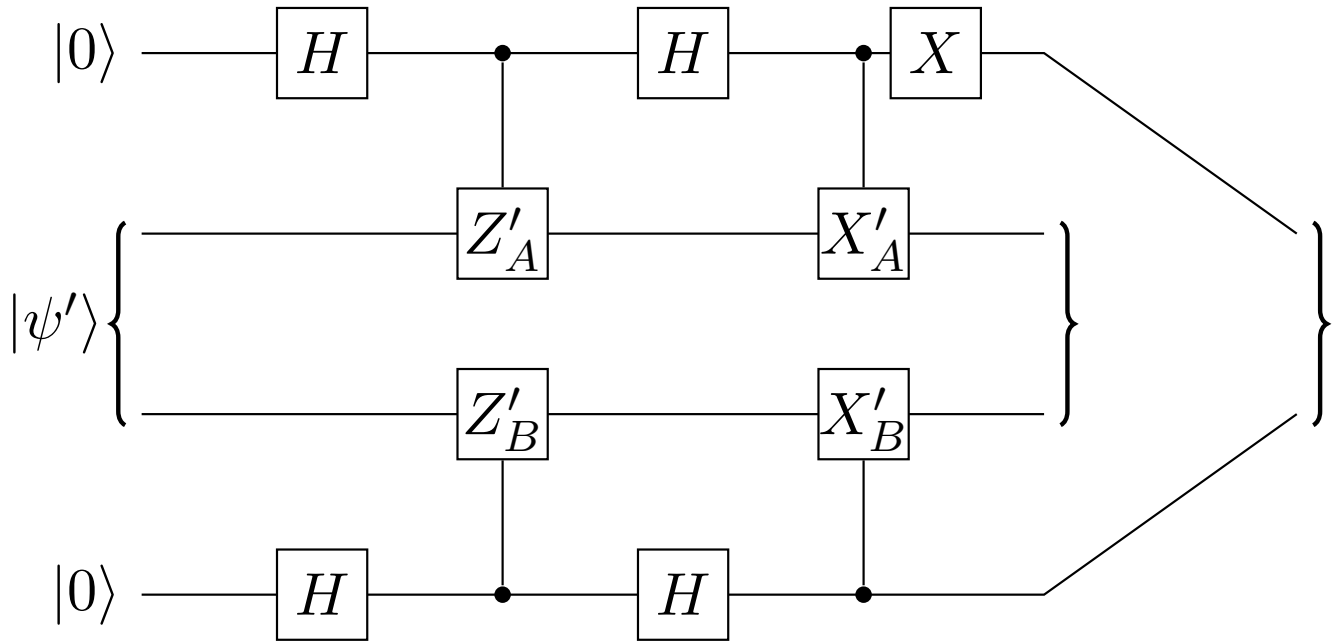
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



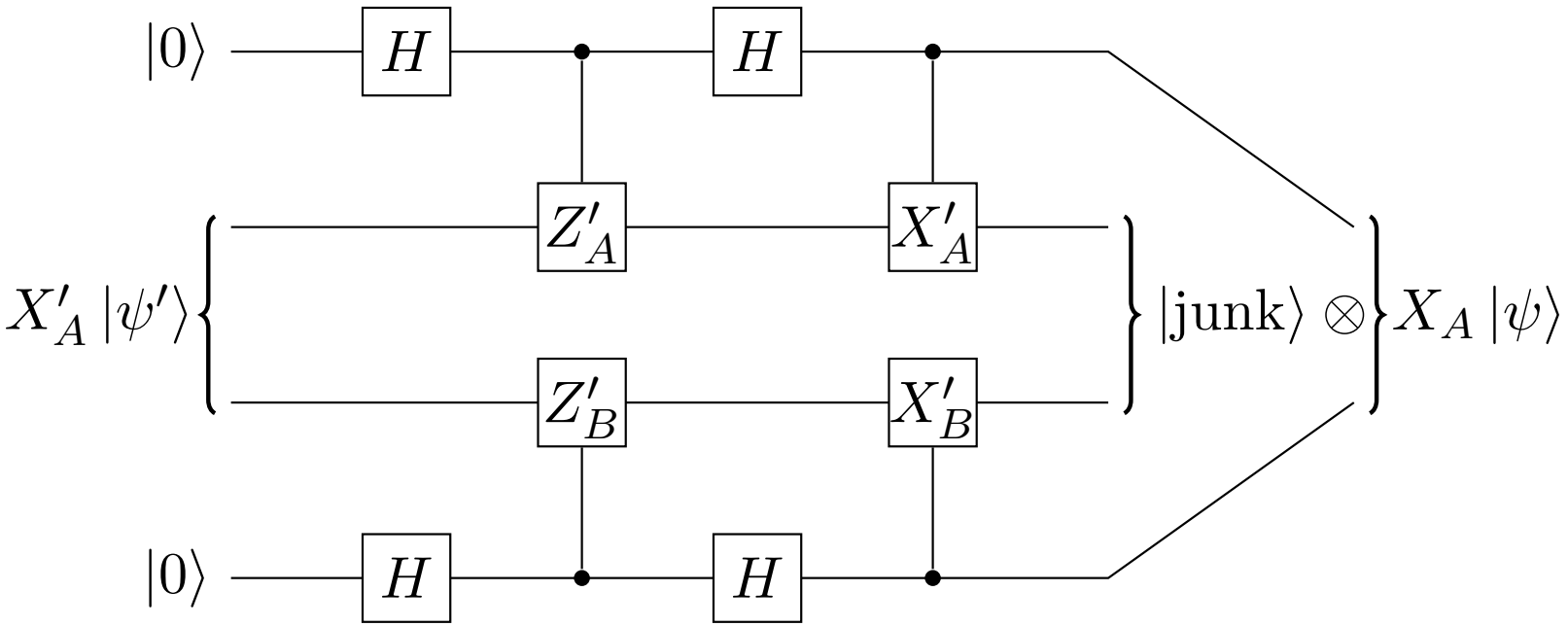
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



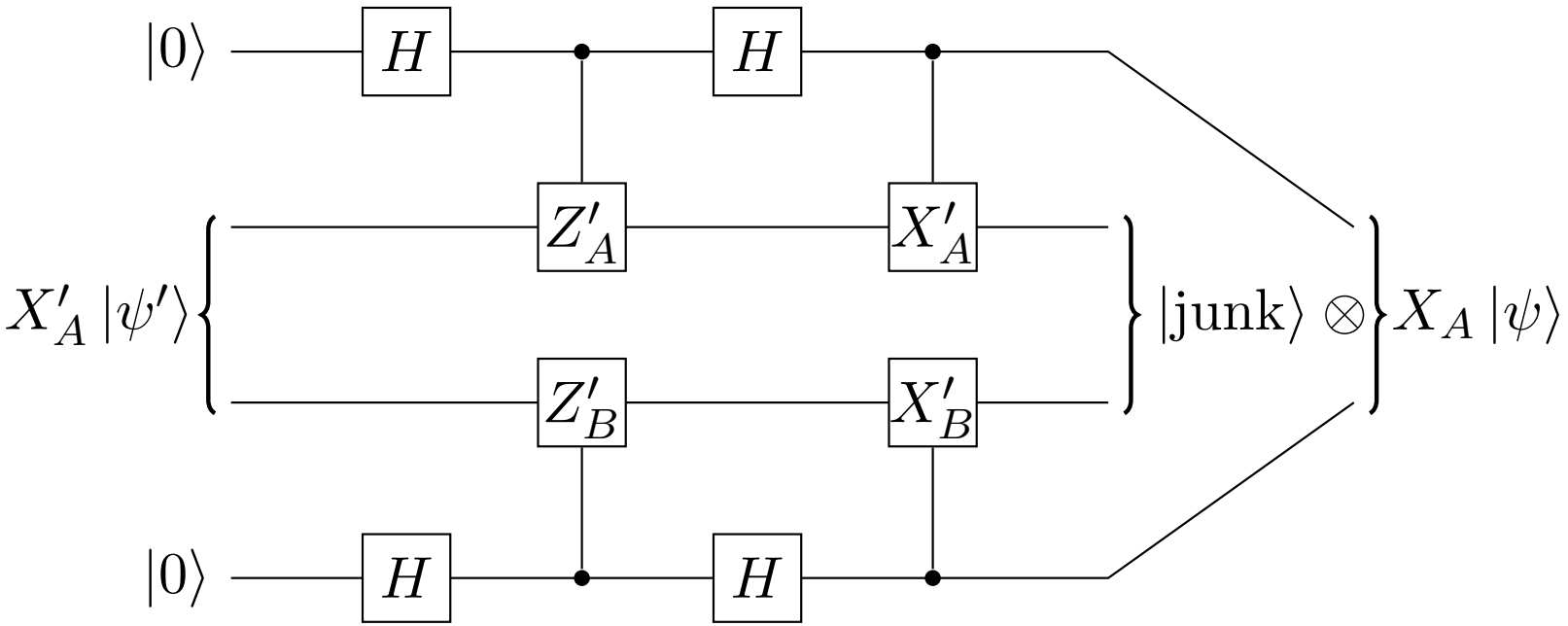
Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



Self-testing X' and Z'

We can now propagate X' and Z' through the isometry and show the equivalence with X and Z acting on the output.



The process for Z' is similar.

Self-testing X' and Z'

We have shown that the state and measurements on the maximally violating black box are equivalent by isometry to the ideal setting of partially entangled qubits.

This result is also robust to noise.

Thank you for your attention!