Nonlocal games, synchronous correlations, and Bell inequalities

Nishant Rodrigues[1,3] and Brad Lackey[1,2,3,4,5]

[1]Joint Center for Quantum Information and Computer Science, University of Maryland
[2]Institute for Advanced Computer Studies, University of Maryland
[3]Department of Computer Science, University of Maryland
[4]Department of Mathematics, University of Maryland
[5]Quantum Systems Group, Microsoft Quantum, Redmond

Overview

We describe a device-independent quantum key distribution (DIQKD) protocol that is symmetric between Alice and Bob using the notion of a *synchronous* correlation. Our analysis uses nonlocal games, $p(y_A, y_B \mid x_A, x_B)$ where $x_A, x_B \in X$ and $y_A, y_B \in Y$ that are synchronous: $p(y_A, y_B|x, x) = 0$ whenever $x \in X$ and $y_A \neq y_B \in Y$.

We show that when $|X| = 2$ and $|Y| = 2$, all synchronous symmetric nonsignaling correlations are classical, and therefore there are no synchronous Bell inequalities. When $|X| = 3, |Y| = 2$ we show there are precisely four synchronous Bell inequalities, each of the form $J_0, J_1, J_2, J_3 \geq 0$, where each J_k is an affine function of the correlation matrix entries. We examine violation of these Bell inequalities and prove a synchronous analogue of Tsirel'son bound: each $J_0, J_1, J_2, J_3 \geq -\frac{1}{8}$.

We extend beyond synchronous correlations and show that there are natural measures of asymmetry, a form of bias, and asychronicity, and these bound the potential synchronous Bell violations realizable by general classical correlations.

A Synchronous QKD Protocol

A single round of the protocol operates as follows:

1. Alice and Bob share an EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. Independently, Alice and Bob randomly select from one of three fixed measurement bases to measure his or her half of the EPR pair.
3. After measurement, Alice and Bob exchange the basis selection they made.
4. If they selected the same basis, they store the output of their measurements as a shared secret value. If they chose differing bases, they exchange their measurement outcomes and store these for later performing a self-test of the device.

Nonlocal games

Two players, Alice and Bob:

- have inputs $x_A, x_B \in X$ and output $y_A, y_B \in Y$;
- may use preshared randomness and quantum resources (e.g. EPR pairs) no communication.

We study nonsignaling nonlocal games based on synchronous correlations.

- A correlation p is *synchronous* if $p(y_A, y_B|x, x) = 0$ whenever $x \in X$ and $y_A \neq y_B \in Y$.
- A *classical* correlation takes the form
$$p(y_A, y_B|x_A, x_B) = \sum_{\omega\in\Omega} \mu(\omega) p_A(y_A|x_A, \omega) p_B(y_B|x_B, \omega)$$
where ω is Alice and Bob's preshared randomness.
- A *quantum* correlation takes the form
$$p(y_A, y_B|x_A, x_B) = \mathrm{tr}((E^{x_A}_{y_A} \otimes F^{x_B}_{y_B})\rho)$$
for $\rho \in \mathfrak{H}_A \otimes \mathfrak{H}_B$ and POVMs $\{E^x_y\}_{y\in Y}$ and $\{F^x_y\}_{y\in Y}$ for each $x \in X$.

Nonsignaling correlations with $|Y| = 2$ are often written in coordinates:
$$a_{x_A} = \sum_{y_A,y_B} (-1)^{(1,0)\cdot(y_A,y_B)} p(y_A, y_B|x_A, x_B)$$
$$b_{x_A} = \sum_{y_A,y_B} (-1)^{(0,1)\cdot(y_A,y_B)} p(y_A, y_B|x_A, x_B)$$
$$c_{x_A,x_B} = \sum_{y_A,y_B} (-1)^{(1,1)\cdot(y_A,y_B)} p(y_A, y_B|x_A, x_B)$$

Synchronous Correlations

Result 1: *A correlation p is symmetric and nonsignaling if and only if (i) $c_{x_A,x_B} = c_{x_B,x_A}$ and (ii) $a_x = b_x$.*

Result 2: *A correlation p is synchronous and nonsignaling if and only if for all $x \in X$ we have (i) $c_{x,x} = 1$ and (ii) $a_x = b_x$.*

Every synchronous classical or quantum correlation is symmetric, but there are synchronous nonsignaling correlations that are not.

Result 3: *When $|X| = 2$ every symmetric synchronous nonsignaling correlation is classical.*

Result 4: *When $|X| = 2$ every synchronous quantum correlation is classical, hence there are no synchronous Bell inequalities in this case.*

Synchronous Bell inequalities

In the case of $X = \{0, 1, 2\}$ and $Y = \{0, 1\}$ we find four synchronous Bell inequalities:
$$J_0 = \tfrac{1}{4}(1 - c_{01} - c_{02} + c_{12}) \geq 0$$
$$J_1 = \tfrac{1}{4}(1 - c_{01} + c_{02} - c_{12}) \geq 0$$
$$J_2 = \tfrac{1}{4}(1 + c_{01} - c_{02} - c_{12}) \geq 0$$
$$J_3 = \tfrac{1}{4}(1 + c_{01} + c_{02} + c_{12}) \geq 0$$

Tsirel'son Bounds and Rigidity

Result 5: *Every synchronous symmetric nonsignaling strategy satisfies $J_0, J_1, J_2, J_3 \geq -\frac{1}{2}$.*

Like CHSH or Magic Square games, we use
$$M_x = E^x_0 - E^x_1$$
which are ± 1-valued observables. Then, e.g.,
$$\mathrm{tr}((M_0 + M_1 + M_2)^2) = 1 + 8J_3.$$

Result 6: *Every synchronous quantum correlation satisfies $J_0, J_1, J_2, J_3 \geq -\frac{1}{8}$.*

Result 7: *For each $k = 0, 1, 2, 3$ there exists a unique synchronous quantum correlation with $J_k = -\frac{1}{8}$.*

For example, $J_3 = -\frac{1}{8}$ for a shared EPR pair and observables:
$$[M_0] = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$[M_1] = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix},$$
$$\text{and } [M_2] = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix}.$$

Rigidity result 7 above leads to a self-test for an EPR pair. This is the basis for a device-independent security proof for the protocol.

Asynchronicity and Asymmetry

Synchronous rigidity of, say, $J_3 = -\frac{1}{8}$ produces a certificate of a maximally entangled state. However, asynchronous protocols can also have $J_3 = -\frac{1}{8}$.

For the security proof we need to bound asynchronicity, asymmetry, and bias defined as follows:
$$A_{j,k} = \frac{1}{2}(c_{j,k} - c_{k,j}) \quad \text{("asymmetry")}$$
$$B_j = a_j - b_j \quad \text{("bias")}$$
$$C_{j,k} = \frac{1}{2}(c_{j,k} + c_{k,j}) \quad \text{(for } j \neq k\text{)}$$
$$S_j = 1 - c_{j,j} \quad \text{("asynchronicity")}$$

Result 8: *Among symmetric classical correlations, at most one of $J_0, J_1, J_2, J_3 \geq 0$ can be violated. Moreover any such violation satisfies $J_j \geq \max\{-\frac{S_0}{4}, -\frac{S_1}{4}, -\frac{S_2}{4}\}$ and this bound is sharp.*

Result 9: *Suppose $\max\{|A_{j,k}|, |B_j|, S_j\} \leq \epsilon$. Then no synchronous Bell violation $J_3 < \frac{\epsilon}{2}$ can come from a (asymmetric, biased, and asynchronous) classical correlation.*

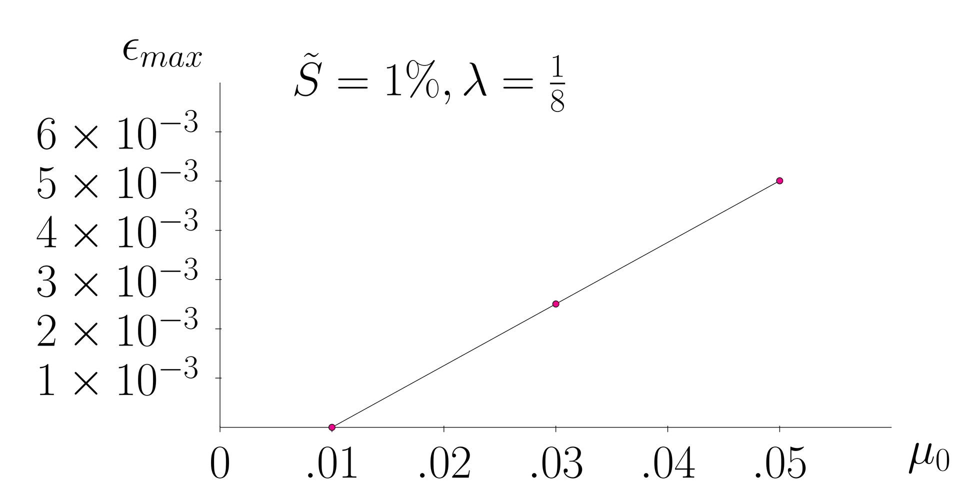
Causality Loophole

Causality Loophole (roughly): maximal Bell violations can be simulated with classical communication.

A new security assumption: Eve has imperfect knowledge of Alice's and Bob's inputs.

Informally, even with unlimited resources, to produce a correlation with $J_3 = -\frac{1}{8}$ and $S \leq \mu_0$ requires Eve have near perfect knowledge of Alice's and Bob's inputs.

We plot the maximum value for Eve's uncertainty ϵ_{max}, for asynchronicity μ_0. Here $\tilde{S} = .01$ is Eve's asynchronicity, and λ is the allowed error in the expected J_3 violation.



Conclusions

1. For $|X| = |Y| = 2$, there are no synchronous Bell inequalities.
2. For $|X| = 3, |Y| = 2$, there are four synchronous Bell inequalities.
3. Maximal synchronous Bell violations are rigid and lead to self-tests of an EPR pair.
4. We obtain a symmetric device-independent quantum key distribution protocol.
5. Proposed a mild security assumption that avoids the "causality loophole" in DIQKD protocols.

arXiv:1707.06200