DEVICE-INDEPENDENT TRIPARTITE QUANTUM KEY DISTRIBUTION FROM THREE-PLAYER QUANTUM GAMES

Second Progress Report

Mahrud Sayrafi

I. Results To Date

In the first progress report we presented the motivation for this project along with a detailed security definition and the adversarial scenario that we want to consider. Further, we introduced an elementary key distribution protocol based on the GHZ-state that satisfied some, but not all, of our goals. In particular, the GHZ-states are highly entangled but fragile with respect to losses, so they could not be used for two-party key distribution if one of the particles was lost due to environmental errors. Since then, we have shifted our focus onto the W-state which is much less entangled but highly robust against losses.

Here we will primarily discuss our work on the W-state along with the methods that we used to look for best strategies. This state, which can be represented in the bra-ket notation as:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

is interesting for us because if we trace out one of the qubits, the reduced state will still exhibit entanglement. We will show the robustness of W-state and fragileness of GHZ-state in section (I.3).

I.1. **The Game.** The first step in using this state is looking for a Bell-type inequality that can be maximally violated by the W-state. For now we will focus on Bell polynomials that represent strategies with two measurements and binary outputs and are symmetric with respect to the parties. One such inequality found by Brunner et al. in Ref. [4] can be written as:

$$\begin{aligned}\langle\beta\rangle = {} & \langle A_0B_0C_0\rangle + \langle A_1B_0C_0\rangle + \langle A_0B_1C_0\rangle + \langle A_0B_0C_1\rangle \\ & -(\langle A_1B_1C_1\rangle + \langle A_0B_1C_1\rangle + \langle A_1B_0C_1\rangle + \langle A_1B_1C_0\rangle) \\ & +\langle A_0B_1I_C\rangle + \langle A_1B_0I_C\rangle + \langle A_0I_BC_1\rangle + \langle A_1I_BC_0\rangle + \langle I_AB_0C_1\rangle + \langle I_AB_1C_0\rangle \leq 6\end{aligned} \tag{1}$$

where we used the shorthand:

$$\langle A_0B_0C_0\rangle = \langle\psi|A_0 \otimes B_0 \otimes C_0|\psi\rangle,$$

$\langle A_iB_jC_k\rangle = \pm 1$ denotes outcome of parties A, B, and C measuring their qubits in i-th, j-th, and k-th measurement setting respectively, and I_A, I_B, and I_C mean measuring using the identity operator. The first two lines of this inequality are also referred to as the Svetlichny's inequality [3]. It can be proven that this inequality cannot be violated by the GHZ-state [4].

I.2. **The Strategy.** A strategy for a quantum game consists of the quantum state along with the measurement settings that can violate the inequality. For this game Brunner et al. gave the optimal measurements to be of the form:

$$A_i = \cos\theta_i Z + \sin\theta_i X$$

where X and Z are Pauli matrices. The optimal violation of the inequality above using the W-state is $\langle\beta\rangle \approx 7.2593$ given by measurements with angles $\theta_0 = 0.2677\pi$ and $\theta_1 = \pi - \theta_0$. However,

Date: July 28, 2014.

the maximal violation was numerically found to be achieved by a slightly modified state $|\psi\rangle = 0.9971|W\rangle - 0.07597|111\rangle$ with measurement angles of $\theta_0 = 0.2615\pi$ and $\theta_1 = \pi - \theta_0$

The next step in the 3-party setting is to find measurements such that all parties achieve the same outcome with at least a high probability. We can then apply key distillation processes such as information reconciliation to find a secure string that can be used as a key.

I.3. **Bipartite Correlations.** Before devising a protocol however, we needed to make sure that the bipartite correlations of W-state can also be used to create a key in case of losing a qubit. The effects of such an event can be represented by tracing out a qubit out of the density matrix. The resulting reduced density matrix is:

$$\rho_{AB} = Tr_C(|W\rangle\langle W|) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2}$$

We can use the Positive Partial Transpose criterion to check that this reduced density matrix is entangled. To do so, we have to show that the partial transpose of this matrix has negative eigenvalues. The partial transpose of ρ_{AB} is:

$$\rho_{AB}^{T_B} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

which in fact has eigenvalues $\{\frac{1}{2} + \frac{\sqrt{5}}{2}, 1, 1, \frac{1}{2} - \frac{\sqrt{5}}{2} \approx -0.62\}$, thus ρ_{AB} is entangled.

As a side note, we can use the same method to show that tracing out one qubit from a GHZ-state will result in the following reduced density matrix:

$$Tr_C(|GHZ\rangle\langle GHZ|) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which is only classically correlated.

Even though we showed that the reduced density matrix of the W-state is entangled, not all entangled correlations are nonlocal. In order for this state to be useful in our protocol we need an inequality that can be violated by it. Note that this state will not maximally violate any inequality. This statement can be proven by looking at the eigendecomposition of ρ_{AB}:

$$\begin{aligned} \rho_{AB} &= \sum \lambda_i |v_i\rangle\langle v_i| \\ &= \frac{2}{3}|\Psi^+\rangle\langle\Psi^+| + \frac{1}{3}|00\rangle\langle 00| \end{aligned} \tag{3}$$

where λ_i and v_i are the eigenvalues and eigenvectors of ρ_{AB}, and $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. This is equivalent to having the Bell state $|\Psi^+\rangle$ with probability $\frac{2}{3}$ and the classical state $|00\rangle$ with probability $\frac{1}{3}$. It can be shown that a mixed state ρ maximally violates an inequality if and only if all of its components (i.e., the states $|v_i>$) violate the inequality maximally, but in this case $|00>$ is a classical state and cannot violate an inequality.

I.4. **The Guessing Game.** The fact that a reduced correlation can never achieve maximal violation does not mean that it cannot lead to a key. The reason is that even with smaller amounts of violation we can have a protocol that only has a lower rate of producing key bits. In our security proof we will use the the fact that the devices are under no-signaling constraints to show that if

Eve, an adversary, has a way of guessing the key bit with a probability higher than a bound, then the no-signaling condition is broken, thus Eve's guessing ability is limited by that bound.

Using linear programming techniques we generated the following table for in which P_w is the probability of winning the CHSH game [6] and P_e is the probability of Eve's guessing ability:

P_w	P_e
0.75	1.00
0.76	0.98
0.77	0.96
0.78	0.94
0.79	0.92
0.80	0.90
0.81	0.88
0.82	0.86
0.83	0.84
0.84	0.82
0.85	0.80

For instance in the first row there is no violation of classical inequality $P_w \leq 0.75$, so Eve has at least one strategy for guessing Alice's output. However, as the non-locality increases, Eve's guessing ability reduces.

II. Methods

In this section we describe the optimization methods that we used to approximate the best strategy (state and measurements) for a Bell inequality. We categorize the inequalities based on three parameters (n, m, Δ) where the number of parties is n, number of measurement settings for each party is m, and number of possible outcomes for each measurement is Δ. As mentioned before, for now we focus only on the cases where the measurements have two possible outcomes; i.e., $\Delta = 2$.

Using the fact that the Pauli matrices X, Y, and Z together with the 2×2 identity matrix I form an orthogonal basis for the real Hilbert space of 2×2 complex Hermitian matrices, we can parametrize our measurements operators in the form:

$$M_j = c_I I + c_X X + c_Y Y + c_Z Z \tag{4}$$

where M_j is the j-th measurement setting and c_j are real coefficients with $c_i^2 + c_x^2 + c_y^2 + c_z^2 = 1$. This decomposition is also known as the Hilbert-Schmidt decomposition. Additionally, in Ref. [4] Brunner et al. claim that the optimal measurement settings for our inequality can always be taken to be real, so we can simplify the parametrization to:

$$M_j = \cos\theta_j Z + \sin\theta_j X \tag{5}$$

where θ_j is an angle from 0 to π and is easier to program.

II.1. Strategy for Tripartite Inequality (3,2,2).

Given an inequality for three parties we need to find the state $|\psi\rangle$ and measurement settings that maximally violate it. Our task is to maximize $\langle\psi|\beta|\psi\rangle$ where β is the Bell inequality in Eq. 1 if we substitute the measurement operators with operators in the form of Eq. 5.

If we let $\mathcal{M}$ be a measurement operator, we know that it has an eigendecomposition of the form:

$$\mathcal{M} = \sum_i \lambda_i |v_i\rangle\langle v_i| \tag{6}$$

where λ_i are the eigenvalues and v_i are the respective eigenvectors (i.e., $\mathcal{M}v_i = \lambda_i v_i$). We have:

$$\begin{aligned}\langle\psi|\mathcal{M}|\psi\rangle &= \sum_i \lambda_i \langle\psi|v_i\rangle\langle v_i|\psi\rangle \\ &= \sum_i \lambda_i \|\langle v_i|\psi\rangle\|\end{aligned} \tag{7}$$

Thus, our problem is to maximize the dot product $\langle v_i|\psi\rangle$ for the eigenvector that has the largest eigenvalue. In addition, since the dot product of two vectors is maximum when the angle between them is zero and $|v_i|\psi\rangle$ and $|\psi\rangle$ are both normalized vectors, the optimal strategy would be to set our state equal to the eigenvector with the largest eigenvalue.

Note that we need to check this for all possible measurement settings. As mentioned before, each measurement can be described in the form of Eq. 5, so we need to run a loop for the angle of each of the six measurements. As a result the computational complexity of this program would be in the order of $\mathcal{O}(n^6)$ where n is the number of angles we check for each measurement. However, in inequalities with $n = 2$, we know that the measurements are symmetric with respect to unitary operations that rotate a qubit. Using that fact we can fix A_0, B_0, and C_0 and run the loop only on the second measurement of each party. This will reduce the complexity to $\mathcal{O}(n^3)$.

II.2. **Strategy for Bipartite Inequality (2,m,2).** Once we have a state $|\psi\rangle$ that satisfies the previous condition, we need to find an inequality and strategy that uses the reduced density matrix $\rho_{AB} = Tr_C(|\psi\rangle\langle\psi|)$.

For simplicity we started by looking at inequalities with $m = 2$. However, in Ref. [5] Brunner et al. show that the CHSH inequality [6] is the only tight Bell inequality for the (2,2,2) case, which means that if there is a strategy that violates a different inequality, then it will also violate the CHSH inequality. Using the same shorthand used in Eq. 1, we can write the CHSH inequality as:

$$\langle CHSH\rangle = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2 \tag{8}$$

Similar to the previous section we need to use run loops on the measurement angles, however, knowing the reduced density matrix ρ_{AB} from previous section, we can group the measurements in the following manner:

$$\langle CHSH\rangle = \langle B_0(A_0 + A_1)\rangle + \langle B_1(A_0 - A_1)\rangle \leq 2 \tag{9}$$

Now if we run two loops for A_0 and A_1, our problem would reduce to maximizing:

$$\begin{aligned}\langle CHSH\rangle &= Tr_{AB}(B_0 \otimes (A_0 + A_1)\cdot\rho_{AB}) + Tr_{AB}(B_1 \otimes (A_0 - A_1)\cdot\rho_{AB}) = \\ &= \sum_{i=\{0,1\}} Tr_{AB}(B_i \otimes X_i \cdot \rho_{AB})\end{aligned} \tag{10}$$

where $X_0 = A_0 + A_1$ and $X_1 = A_0 - A_1$ are known. Next, we can use partial trace to trace out qubit A:

$$\begin{aligned}\sum_{i=\{0,1\}} Tr_{AB}(B_i \otimes X_i \cdot \rho_{AB}) &= \sum_{i=\{0,1\}} Tr_B(B_i \cdot Tr_A(X_i \otimes I_B \cdot \rho_{AB})) \\ &= \sum_{i=\{0,1\}} Tr_B(B_i \cdot Z_i)\end{aligned} \tag{11}$$

where $Z_i = Tr_A(X_i \otimes I_B \rho_{AB})$ are known. At this point, we can use Hilbert-Schmidt decomposition to rewrite the 2×2 matrices B_i and Z_i as:

$$\begin{aligned}B_i &= b_I I + b_X X + b_Y Y + b_Z Z \\ Z_i &= z_I I + z_X X + z_Y Y + z_Z Z\end{aligned} \tag{12}$$

where b_j and z_j are real coefficients with $\sum_j b_j^2 = \sum_j z_j^2 = 1$. Using this decomposition, we can rewrite the traces as:

$$\sum_{i=\{0,1\}} Tr_B(B_i \cdot Z_i) = \sum_{i=\{0,1\}} \bar{b} \cdot \bar{z} \tag{13}$$

Thus, the problem is again reduced to maximizing a bounded dot product which means the optimal value is achieved when:

$$\bar{b} = \bar{z}$$

so:

$$\begin{aligned} B_0 &= Tr_A((A_0 + A_1) \otimes I_B \rho_{AB}) \\ B_1 &= Tr_A((A_0 - A_1) \otimes I_B \rho_{AB}) \end{aligned} \tag{14}$$

Unfortunately, however, we found out that the reduced density matrix that we found in Sec. (1.3) does not violate the CHSH inequality. Thus, we needed to look into (2,3,2) inequalities. Much of the progress in this path remains to be done, but we wrote a similar program that given a reduced density matrix ρ_{AB}, runs three loops for measurement angles of A_0, A_1, and A_2, and optimizes B_0, B_1, and B_2. In the next section we describe our plans for using this program.

III. Plans

Our main plan for the remainder of the program is to first look for suitable (2,3,2) inequalities such as the ones mentioned in Ref. [8]. If that path didn't succeed, we have to look for other (3,2,2) inequalities and other strategies which would likely mean abandoning the W-state. In that case, we would start by looking for better (3,2,2) inequalities such as the ones listed in Ref. [7].

Further, we will finish testing and optimizing the programs and eventually connecting them together as modules to create a larger search program that looks for different (3,2,2) inequalities, calculates the strategy with maximal violation, computes the bipartite reduced density matrix equivalent to its state, and look for inequalities that can be violated by that.

If that fails as well, we will begin to think about whether we can prove a no-go theorem stating that non-locality cannot be found in both an entangled tripartite state and its bipartite reduced density matrix.

References

[1] W. Dur, G. Vidal, and J. I. Cirac; "Three qubits can be entangled in two inequivalent ways" Physics Review, A 62, 062314 (2000) arXiv:quant-ph/0005115

[2] W. Dur; "Entanglement molecules" arXiv:quant-ph/0006105

[3] G. Svetlichny; "Distinguishing three-body from two-body nonseparability by a Bell-type inequality" Phys. Rev. D 35. 3066 (1987)

[4] N. Brunner, J. Sharam, T. Vertesi; "Testing the Structure of Multipartite Entanglement with Bell Inequalities" arXiv:1110.5512 [quant-ph]

[5] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner; "Bell nonlocality" arXiv:1303.2849 [quant-ph]

[6] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt; "Proposed Experiment to Test Local Hidden-Variable Theories" Physical Review Letters, Vol. 23, No. 15, American Physical Society, October 1969, pp. 880-884 doi:10.1103/PhysRevLett.23.880

[7] C. Sliwa; "Symmetries of the Bell correlation inequalities" arXiv:quant-ph/0305190

[8] D. Collins, N. Gisin; "A Relevant Two Qubit Bell Inequality Inequivalent to the CHSH Inequality" arXiv:quant-ph/0306129