CHSC858F Final Project Presentation

1

1

Rushil Dandamudi | December 8, 2022

Background

The CHSH Game Clauser, Horne, Shimony, Holt: 1969 | APS Alice \mathcal{X} Û



 $x \wedge y \stackrel{?}{=} a \oplus b$

The CHSH Game Clauser, Horne, Shimony, Holt: 1969 | PRA

Game Value

- Classical = .75
- Quantum = .85

Complexity Theory Ties

- Non-local games ← Graph coloring
- RG informing about BQP vs P



Tsirelson's Inequality .85 is optimal for quantum players | Rigidity of CHSH

$|S_q| = |\langle X_1Y_1 \rangle + \langle X_1Y_2 \rangle + \langle X_2Y_1 \rangle - \langle X_2Y_2 \rangle | \le 2\sqrt{2}$

Tsirelson's Inequality .85 is optimal for quantum players | Rigidity of CHSH

$|S_q| = |\langle X_1Y_1 \rangle + \langle X_1Y_2 \rangle + \langle X_2Y_1 \rangle - \langle X_2Y_2 \rangle | \le 2\sqrt{2}$

$V(G_q) = \frac{1}{2}(1 + \frac{|S|}{4}) \to \frac{1}{2} + \frac{1}{2\sqrt{2}} = .85$

Formula relates sum of expected measurement correlations to Referee's game challenge

Tsirelson 1980 | Letters in Mathematical Physics

Tsirelson's Inequality

.85 is optimal for quantum players | Rigidity of CHSH $|S_a| = |\langle X_1Y_1 \rangle + \langle X_1Y_2 \rangle + \langle X_2Y_1 \rangle - \langle X_2Y_2 \rangle | \le 2\sqrt{2}$

CHSH Inequality shows $|S_c| \le 2$ which results in .75



7

Interactive Proofs of Quantumness from CHSH

CHSH-based iPoQ (iPoQ-2) Kahanamoku-Meyer et al.

- Constructs single-player game for a Proof of Quantumness
 - "Computational Bell Test"
 - Alice is replaced by a cryptographic construction (TCF)



CHSH-based iPoQ (iPoQ-2) Kahanamoku-Meyer, Choi, Vazirani, Yao 2021 | Nature Physics

- Security: hardness reduction from
 - 1. Claw-Free assumption: Winning Classical Adv \rightarrow TCF Adv
 - 2. CHSH: assumed, not proven Gap of .10 is shown



Reducing G-2222 to Completing security proof for i

- Winning Classical Adversary
 CHSH adversary
- Let (P-2,V-2) encapsulate an iPoQ-2 protocol
 - Both parties are classical
 - $P[pass] \approx .85$

iPoQ-	-2
PoQ-2	

$ \psi\rangle$		10100111100 11010110011 11101100100 10011000011
Prover (quantum)		veriner (classical)
Round 1 2. Generate state $\sum_{x} x\rangle_{x} f_{i}(x)\rangle_{y}$	\blacktriangleleft	1. Sample $(f_i, t) \leftarrow Gen(1^n)$
3. Measu State y register can be discarded	y	4. Using trapdoor t compute x_0 and x_1
If preimage requested:	choice	5. Randomly choose to request a preimage or continue
6a. Projectively measure \times register, yielding x	x	7a. If $x \in \{x_0, x_1\}$ return Accept
Otherwise, continue:		Sending x
Round 2 7b. Add one ancilla b; use CNOTs to compute $ r \cdot x_0\rangle_{\scriptscriptstyle L} x_0\rangle_{\scriptscriptstyle L} + r \cdot x_1\rangle_{\scriptscriptstyle L} x_1\rangle_{\scriptscriptstyle L}$ where	≺	6b. Choose random bitstring r
8b. M Alice's Measuremetry yielding a string d. Discard x, state is now $ \psi\rangle_{b} \in \{ 0\rangle, 1\rangle, +\rangle, -\rangle\}$	ent (a) 	9b. Using $r_{\rm c} r_{\rm b} r_{\rm c} d$ determine $ \psi\rangle_{\rm b}$
· · · · · · · · · · · · · · · · · · ·		Sending y
Round Bob's Measureme $(\cos(\frac{\theta}{2}) 0\rangle + \sin(\frac{\theta}{2}) 1\rangle)$	ent (b) ——	10b. Choose random $\theta \in \{\frac{\pi}{4}, -\frac{\pi}{4}\}$
$\left\{ \cos\left(\frac{\theta}{2}\right) 1\rangle - \sin\left(\frac{\theta}{2}\right) 0\rangle \right\}, \text{ yielding a bit } b$	<i>b</i>	11b. If b was likely given $\left \psi\right\rangle_{b}$ return Accept





Reducing G-2222 to iPoQ-2 **Completing security proof for iPoQ-2**

- Referee R will construct Alice and Bob to play G-2222 nonlocally
 - 1. Alice and Bob decide strategy S
 - 2. Alice sends P-2 TCF f and receives f(x) from P-2
 - 3. Alice receives r from V-2 and sends to P-2
 - 4. Alice receives d from P-2
 - 5. b := P-2 final output
 - 6. $a := (r \cdot (x_0 \oplus x_1))(d \cdot (x_0 \oplus x_1) + (1 r \cdot (x_0 \oplus x_1))(r \cdot x_0))$

$ \psi angle$ Prover (quantum)		10100111100 11010110011 11101100100 10011000011 Verifier (classical
Round 1	f_i	1. Sample $(f_i, t) \leftarrow Gen(1^n)$
2. Generate state $\sum_{x} x\rangle_{x} f_{i}(x)\rangle_{y}$	←	
3. Measure y register, yielding bits State is now $(x_0\rangle + x_1\rangle)_{\times} y\rangle_{y}$; y register can be discarded	Prepara	4. Using trapdoor t compute x_0 a
If preimage requested:	choice	5. Randomly choose to request a or continue
6a. Projectively measure \times register, yielding x	x	7a. If $x \in \{x_0, x_1\}$ return Accept
Otherwise, continue:		
Round 2	r	6b. Choose random bitstring r
7b. Add one ancilla b ; use CNOTs to compute $ r \cdot x_0\rangle_{\mathbf{b}} x_0\rangle_{\mathbf{x}} + r \cdot x_1\rangle_{\mathbf{b}} x_1\rangle_{\mathbf{x}}$ where	•	Sonding v
Alice's Measureme	nt (a)	Sending X
$\left \psi ight angle_{b}\in\left\{\left 0 ight angle,\left 1 ight angle,\left + ight angle,\left - ight angle ight\}$	→ (CC)	9b. Using r, x_0, x_1, d , determine $ \psi $
·		Conding
Bob's Measuremer	nt (b)	JUB Senaing y
$\left\{\cos\left(\frac{\theta}{2}\right) 1\rangle - \sin\left(\frac{\theta}{2}\right) 0\rangle\right\}, \text{ yielding a bit } b$		11b. If b was likely given $\left \psi\right\rangle_{b}$ retu





Referee R will construct Alice and Bob to play G-2222 nonlocally



Referee R will construct Alice and Bob to play G-2222 nonlocally



Reducing G-2222 to iPoQ-2 Completing security proof for iPoQ-2

Alice

1. TLF Prep 2. Alice Measure

Nonlocal:

- **1.** Alice and Bob's inputs are random
- 2. Outputs only depend on randomness and computational secret

V-2



Reducing G-2222 to iPoQ-2 Extra whiteboard space



What about larger inputs?





Generalized Inequalities Wehner 2006. | PRA

• With 1 of n possible values, each player can choose 1 of n measurements

General Sum
$$|S| = |\sum_{i=1}^{n} \langle X_i Y_i \rangle$$

 $> + \sum_{i+1}^{n-1} < X_{i+1}Y_i > - < X_1Y_n > |$ i=1

 $S_c \le 2n - 2$ $S_q \le 2n \cos(\frac{\pi}{2n})$





The 3-Input CHSH Game (G_{3322})

Game Value

- Classical = .78
- Quantum = .93



The Generalized CHSH Game (G_{3322})

<u>Game Value**</u> • Classical = $.78 = \frac{1}{2}(1 + \frac{5}{9})$ • Quantum = $.93 = \frac{1}{2}(1 + \frac{9\cos(\pi/6)}{9})$

**Assuming all inputs are uniformly distributed and control over distribution of a and b



CHSH-based iPoQ (iPoQ-3) Using 3-to-1 TCFs

• Possible States: $\{0, \pm \frac{\pi}{7}\}$

• Not ideal (cannot reach .93)

• Best Measurements: $\{0, \pm .16\pi\}$

• Computed using SDP

- Completeness: .84
- Soundness: .56



Reducing G-3322 to iPoQ-3 Security proof for iPoQ-3

- Winning Classical Adversary → G-3322 Adversary
- Let (P-3,V-3) encapsulate an iPoQ-3 protocol
- Using the same structure of first reduction, proof follows WLOG
 - G-3322 states match candidate states from TCF
 - P-3 measurements match Bob's



