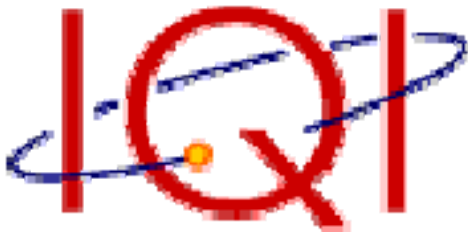


Monogamy of nonlocal quantum correlations

Ben Toner

Institute for Quantum Information and
Department of Physics
Caltech

*IQI/CPI Workshop on Classical & Quantum Information Security
17 December, 2005*



Monogamy of entanglement



Alice



Bob



Charlie

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

$$\rho_{ABC} = |\psi\rangle_{AB} \langle\psi|_{AB} \otimes \rho_C$$

1. Can make this quantitative [CoffmanKunduWootters00], [OsborneVerstraete04];
2. Related to security of quantum key distribution, e.g. Ekert scheme [Ekert91].



Classical correlations are **not** monogamous



Alice



Bob



Charlie

1. The parties share randomness λ .
2. Each party has 0,1 random variables:

$$\{A_i\}$$

$$\{B_j\}$$

$$\{C_k\}$$

that depend on λ and also private randomness.

Joint distribution of AB: $\Pr(A_i \wedge B_j) = \sum_{\lambda} A_i(\lambda)B_j(\lambda)$
does not restrict joint distribution of AC (except for the trivial requirement the marginals $\Pr(A_i)$ are consistent).

Classical correlations are not monogamous



Monogamy of quantum correlations nonlocal



Alice



Bob



Charlie

1. The parties share a quantum state ρ_{ABC} .
2. Each party has ± 1 -valued observables:

$$\{\mathbf{A}_i\}$$

$$\{\mathbf{B}_j\}$$

$$\{\mathbf{C}_k\}$$

Joint distribution of AB: $\langle \mathbf{A}_i \mathbf{B}_j \rangle = \text{tr}(\rho_{ABC} \mathbf{A}_i \otimes \mathbf{B}_j)$
can restrict which joint distributions of AC are allowed.

A prerequisite:

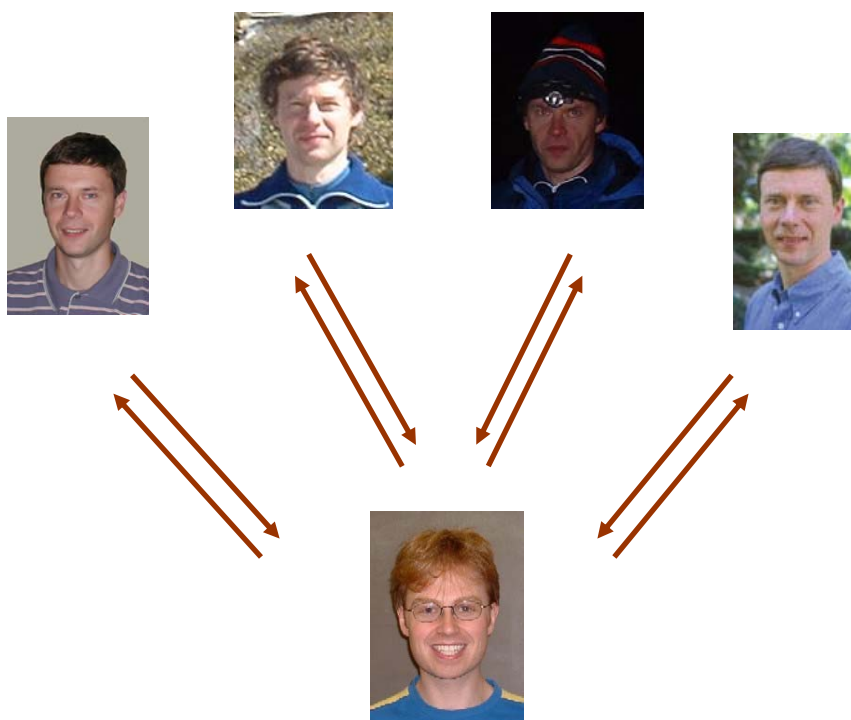
Correlations cannot have a classical description.

Goal

Make this observation quantitative.

Applications

1. Cryptography
2. Interactive proof systems with entangled provers



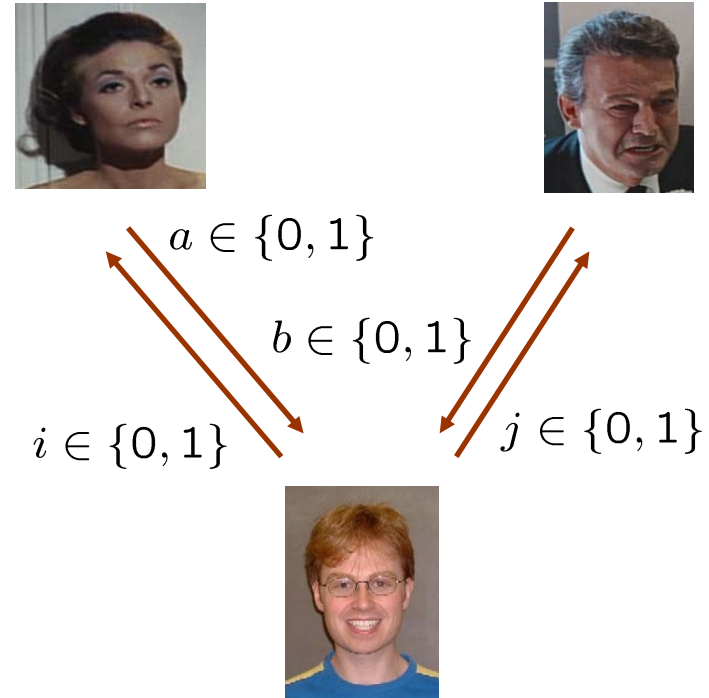
Allowing the provers to share entanglement can affect the soundness of certain proof systems.

[CleveHøyerT.Watrous04]

Nonlocal games: CHSH game

The CHSH game G_{CHSH} is defined as follows:

1. Alice and Bob agree on a strategy. They separate.
2. We choose two bits i and j uniformly at random, and send i to Alice and j to Bob.
3. Alice responds with a bit a and Bob a bit b .
4. They win if $a \oplus b = i \wedge j$.



- Write winning probability of particular strategy as

$$\frac{1}{2} + \frac{1}{8} \langle \mathcal{B}_{CHSH} \rangle$$

- **Classical** value $\omega_c(G_{CHSH}) = 1/2 + 2/8 = 3/4$.
- **Quantum** value $\omega_q(G_{CHSH}) = 1/2 + 2\sqrt{2}/8 \approx 0.85$.

Bell Inequality violation

$$\langle \mathcal{B}_{CHSH} \rangle_c \leq 2$$

$$\max \langle \mathcal{B}_{CHSH} \rangle_q = 2\sqrt{2}$$

Monogamy of CHSH correlations

Theorem: Suppose three parties, A, B, and C share any quantum state ρ (of arbitrary dimension) and each chooses to measure one of two observables. Then

$$\left| \langle \mathcal{B}_{\text{CHSH}}^{\text{AB}} \rangle \right| + \left| \langle \mathcal{B}_{\text{CHSH}}^{\text{AC}} \rangle \right| \leq 4.$$

[Suggested by Michael Nielsen.]

$$\langle \mathcal{B}_{\text{CHSH}}^{\text{AB}} \rangle = \text{tr} (\rho [\mathbf{A}_0 (\mathbf{B}_0 + \mathbf{B}_1) + \mathbf{A}_1 (\mathbf{B}_0 - \mathbf{B}_1)])$$

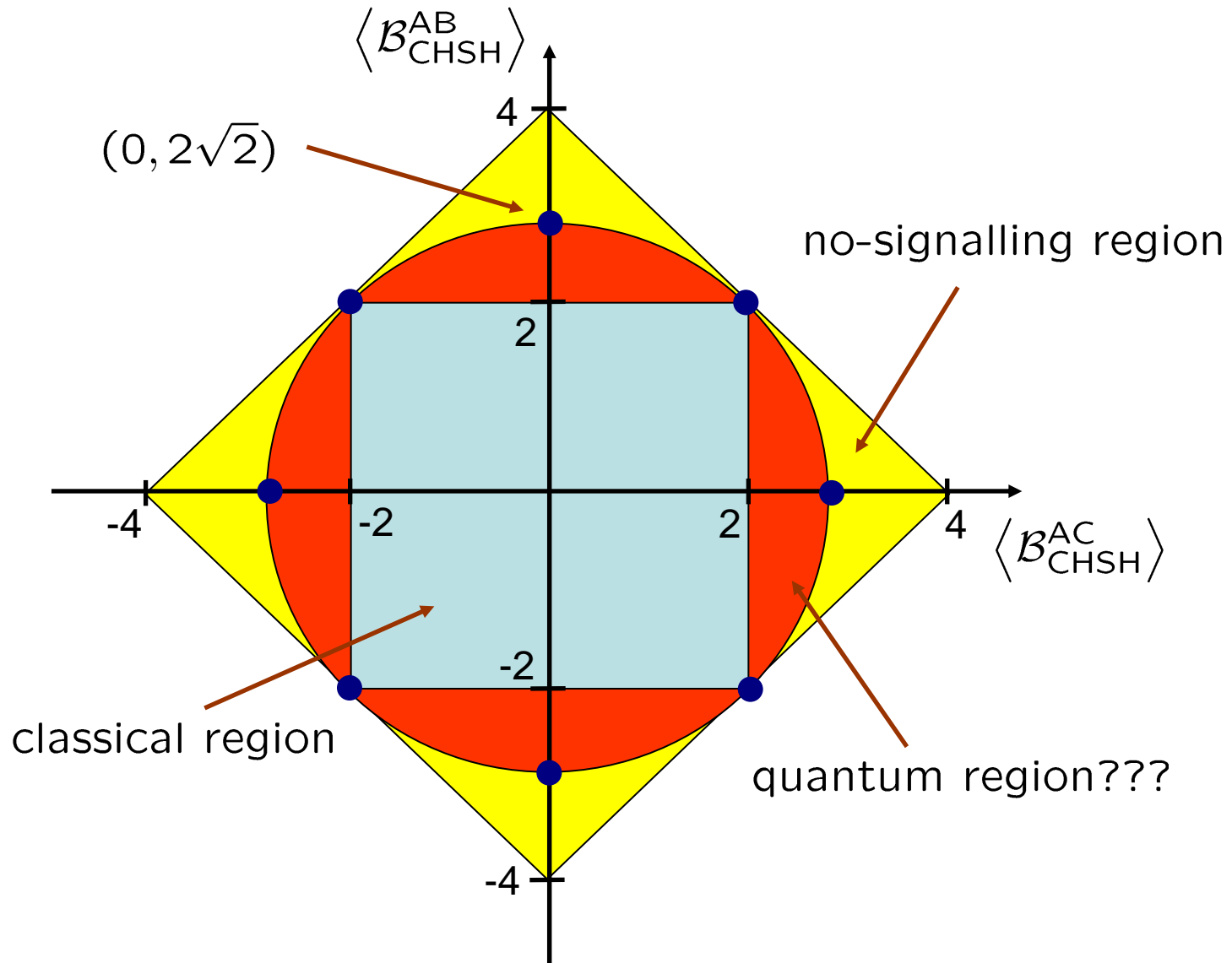
$$\langle \mathcal{B}_{\text{CHSH}}^{\text{AC}} \rangle = \text{tr} (\rho [\mathbf{A}_0 (\mathbf{C}_0 + \mathbf{C}_1) + \mathbf{A}_1 (\mathbf{C}_0 - \mathbf{C}_1)])$$

Corollary: Suppose $N + 1$ parties A, B_1, B_1, \dots, B_N share a quantum state and each chooses to measure one of two observables. Then A violates the CHSH inequality with at most one of the B_i .

Technique

- Generally, hard to obtain bounds on the quantum value of a nonlocal game.
- Quantum correlations are no-signalling.
- So relax to no-signalling probability distributions.
- Determining the no-signalling value of a nonlocal game can be formulated as a linear program.
- For appropriate 3 party version of CHSH game, construct solution to dual program to get bound.

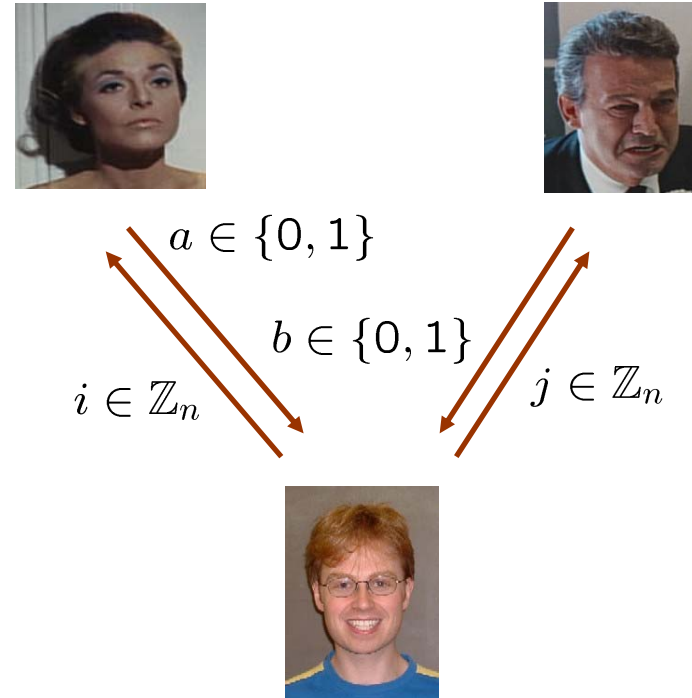
Monogamy of CHSH correlations



Odd cycle game

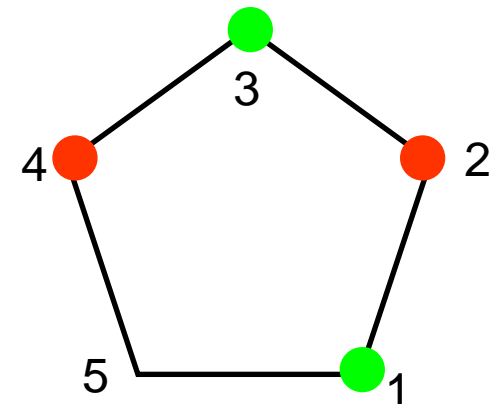
The **odd cycle game** G_{OC} is defined as follows:

1. We choose an integer $i \in \mathbb{Z}_n$ and send it to Alice. With probability $1/2$ we send $j = i$ to Bob, with probability $1/2$ we send $j = i + 1 \pmod n$.
2. Alice responds with a bit a and Bob a bit b .
3. They win if $a \oplus b = [i \neq j]$.

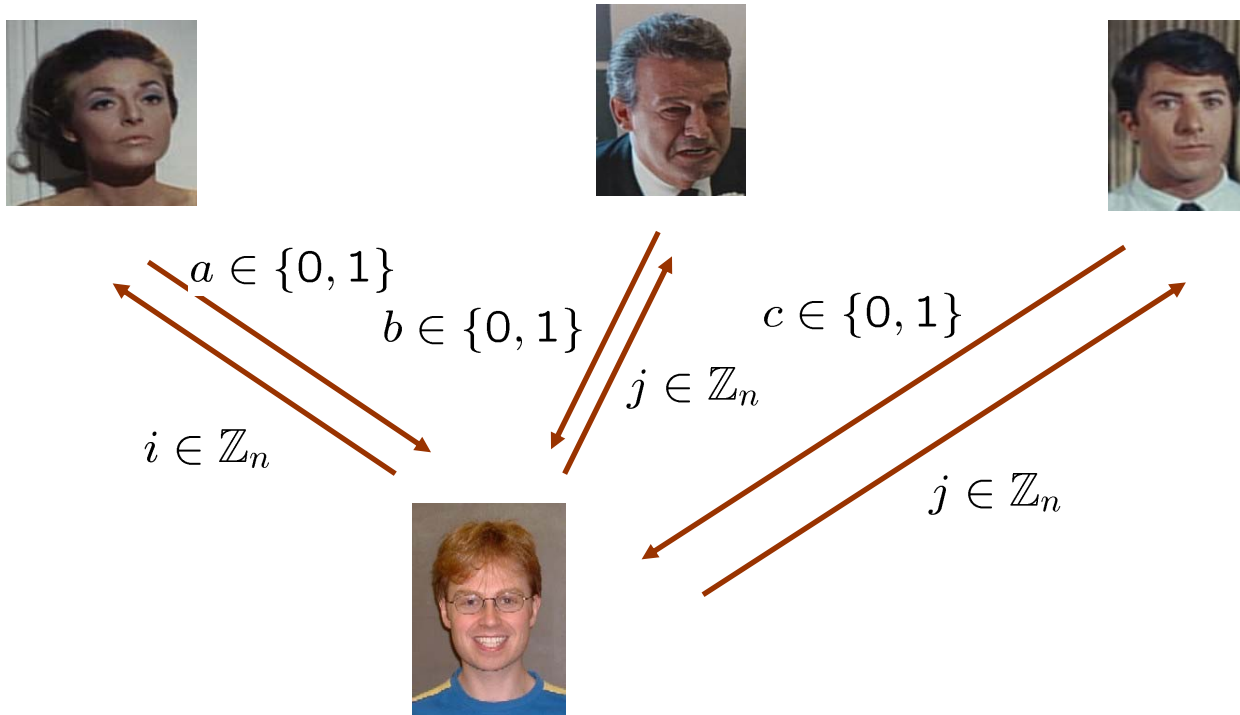


- **Classical** value $\omega_c(G_{OC}) = 1 - \frac{1}{2n}$.
- **Quantum** value $\omega_q(G_{OC}) = \cos^2(\pi/4n) \approx 1 - O(\frac{1}{n^2})$.

[CleveHøyerT.Watrous04]



Modified odd cycle game



- Send B's question to additional prover Charlie.
- Players win if (i) A and B win original game, and (ii) B and C agree.

- **Classical** value $\omega_c(G'_{OC}) = 1 - \frac{1}{2n}$.

- **Quantum** value $\omega_q(G'_{OC}) = 1 - \frac{1}{2n}$.

These correlations are same as those used in cryptographic scheme [BarrettHardyKent04].

Conclusions

- Described new technique to find Tsirelson bounds on the quantum value of a nonlocal game.
- Demonstrated how to use this technique to quantify the monogamy of quantum correlations.



One word:
plastics



One word:
plastics



One word:
plastics