Measurement-device-independent verification of quantum steering via a quantum referee

OR

Verifying ye olde entanglement in the absence of trust

Centre for Quantum Dynamics

Sacha Kocsis, Michael Hall, Adam Bennet, Dylan Saunders & Geoff Pryde

Verifying entanglement in the absence of trust

– with or without Bell violation!

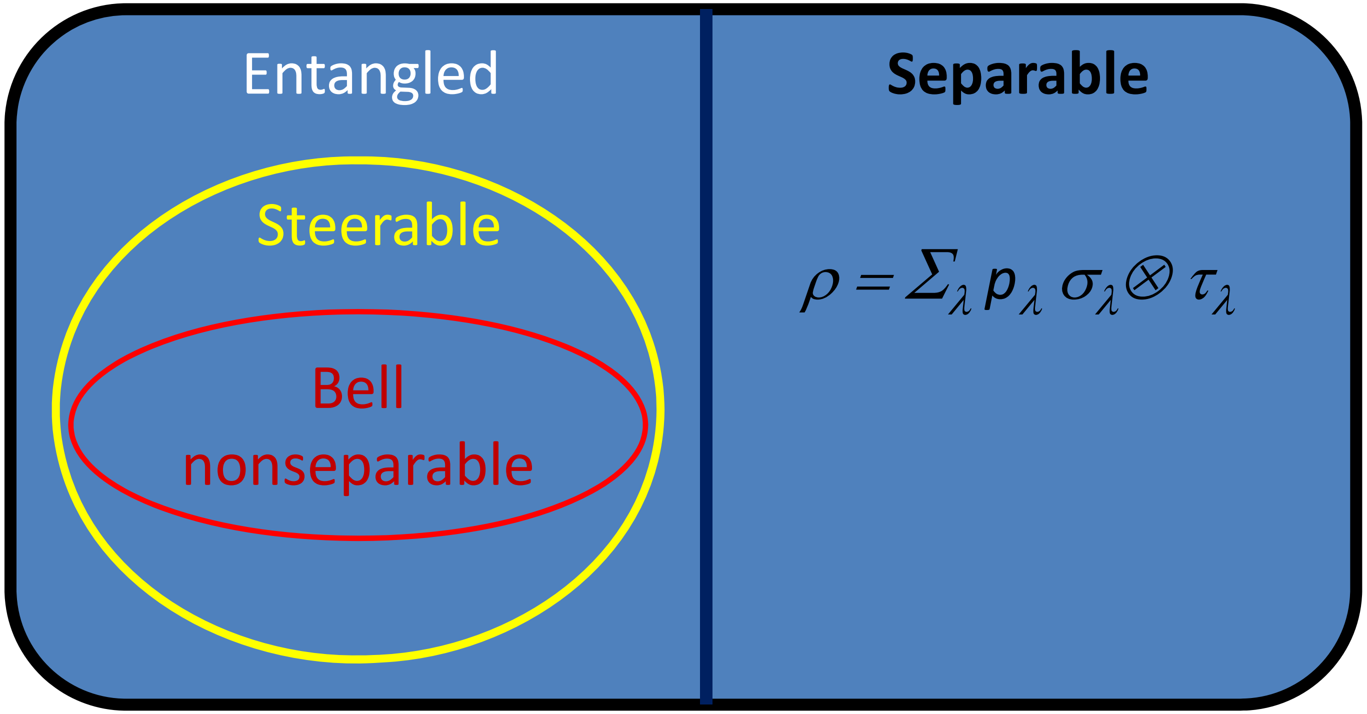
Griffith UNIVERSITY
Centre for Quantum Dynamics

Sacha Kocsis, Michael Hall, Adam Bennet, Dylan Saunders, & Geoff Pryde

Outline

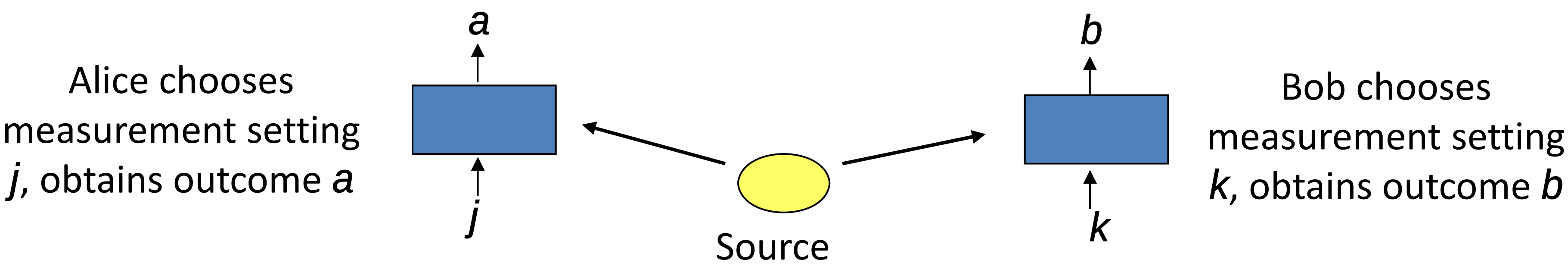
- Degrees of quantum entanglement
- Entanglement games and trust
- Replacing trust by quantum refereeing
  (measurement-device-independence)
- Experiment: quantum-refereed steering game

Degrees of entanglement



- Separable: *local quantum model for correlations*
- Entangled: *no local quantum model* (potential resource)
- **Steerable**: *no local model which is quantum for Bob* (stronger resource)
- **Bell nonseparable**: *no local model* (truly cool resource)

Defining degrees of entanglement



Obtain set of measured joint correlations { $p(a,b|j,k)$ }.

- **ENTANGLED**: *no local quantum model of correlations*

  $p(a,b|j,k) \neq \Sigma_\lambda\, p_\lambda\, p_Q(a|j,\lambda)\, p_Q(b|k,\lambda)$ $\Rightarrow$ *whole greater than parts*

  [with $p_Q(a|j,\lambda) = \mathrm{tr}[\rho_\lambda E_{a|j}]$ for some state ρ_λ and POVM $\{E_{a|j}\}$].

- **STEERABLE**: *no local model which is quantum for Bob*

  $p(a,b|j,k) \neq \Sigma_\lambda\, p_\lambda\, p(a|j,\lambda)\, p_Q(b|k,\lambda)$ $\Rightarrow$ *Alice can steer Bob's state*

- **BELL NONSEPARABLE**: *no local model*

  $p(a,b|j,k) \neq \Sigma_\lambda\, p_\lambda\, p(a|j,\lambda)\, p(b|k,\lambda)$ $\Rightarrow$ *spooky action at distance*

Example: Degrees of entanglement for two-qubit Werner states

Mixture of singlet state and maximally-mixed state:

$$\rho = W\,|\Psi^-\rangle\langle\Psi^-| + (1-W)\ \tfrac{1}{4}\,1\otimes 1$$

a) $W \leq 1/3$: separable

b) $W > 1/3$: entangled (e.g., channel discrimination)

c) $W > 1/2$: steerable (e.g, 1-sided secure QKD)

d) $W > 1/\sqrt{2}$: Bell nonseparable (e.g., 2-sided secure QKD)

Examples of entanglement tests

Bell nonseparability (no local model)

If local model predicts $a_j = \pm 1$, $b_k = \pm 1$, with $j, k = 1,2$

then $a_1 b_1 + a_1 b_2 + a_2 b_1 - a_2 b_2 = \pm 2$.

$\therefore \ |\langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle| > 2 \ \Rightarrow$ Bell nonseparable

Steerability (no local quantum model for Bob)

If $a_j = \pm 1$, and $b_k = \pm 1$ is outcome of measuring spin component` σ_k ,

then Bob's operator $a_1 \sigma_1 + a_2 \sigma_2 = \pm\sigma_1 \pm\sigma_2$ has eigenvalues $\pm\sqrt{2}$.

$\therefore \ |\langle a_1 \sigma_1 \rangle + \langle a_2 \sigma_2 \rangle| > \sqrt{2} \ \Rightarrow$ Alice can steer Bob

Entanglement (no local quantum model for either)

$|\langle \sigma_1 \otimes \sigma_1 \rangle + \langle \sigma_2 \otimes \sigma_2 \rangle| > 1 \ \Rightarrow$ entanglement

Entanglement and trust

- What if Alice and Bob report entanglement – e.g., violation of a suitable inequality – but they (or their government-supplied apparatuses) are not trustworthy?

- Can a referee, Charlie, reliably determine if Alice and Bob in fact do share entanglement?

- It will be assumed that Alice and Bob cannot communicate with each other during the testing stage, although they may have conspired beforehand.

Entanglement and trust: **cheating**

Charlie

Bob & Alice

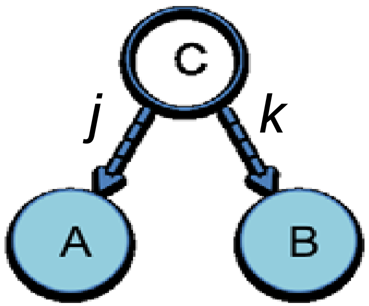
Entanglement and trust: **cheating**

- Alice and Bob claim to have two entangled qubits
- Charlie sends Alice j=1 or 2, and sends Bob k=1 or 2.
- They (or their measurement apparatus) claim to measure $a_j = \sigma_j = \pm 1$ and $b_k = \sigma_k = \pm 1$, respectively, and send the results to Charlie
- In fact, they simply send back the same values from a pre-shared list, such as { 1, 1, -1, 1, -1, 1, -1, -1, -1, …}
- Charlie uses these values to incorrectly calculate:

$$|\langle \sigma_1 \otimes \sigma_1 \rangle + \langle \sigma_2 \otimes \sigma_2 \rangle| = 2 > 1 \Rightarrow \text{ entanglement!}$$

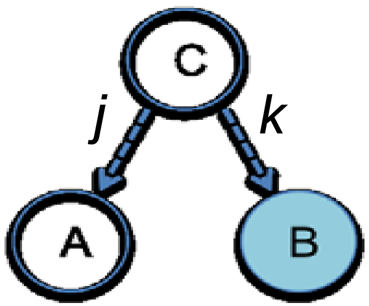
$$|\langle a_1 \sigma_1 \rangle + \langle a_2 \sigma_2 \rangle| = 2 > \sqrt{2} \Rightarrow \text{ steering!}$$

The old picture of trust



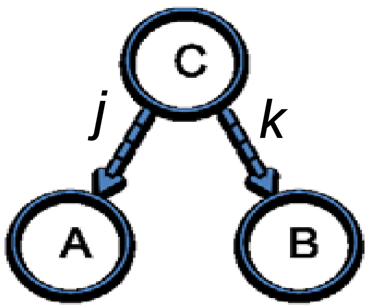
Entanglement

Charlie must trust both Alice and Bob – even if he specifies the settings



Steering

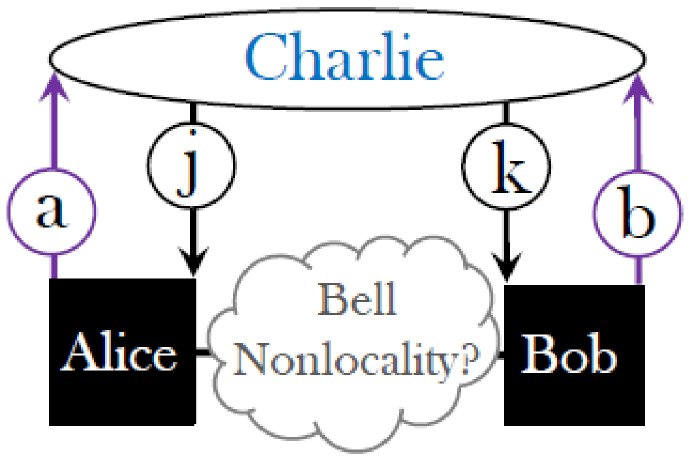
Charlie must trust Bob



Bell nonseparability

No trust necessary if Charlie specifies the measurement settings

Entanglement and trust: Bell nonseparability



Charlie:

- sends input signals, **j** and **k**
- receives output signals, **a** and **b**
- checks if the correlations violate a **Bell inequality**

<u>Advantages</u>

✓ No trust required (black boxes)

✓ Strong entanglement, useful for secure QKD, randomness generation, ….

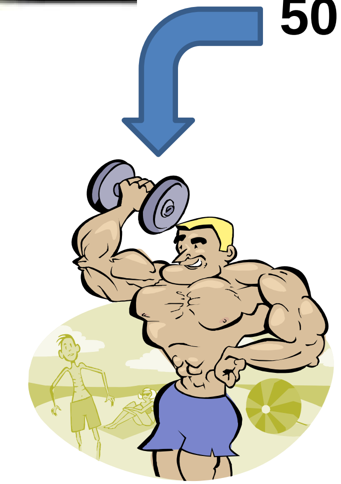
<u>Disadvantage</u>

❖ Not robust over long distances (detection loophole)

Entanglement and trust: **Steerability**

Charlie:

- sends input signals, **j** and **k**
- receives output signals, **a** and **b**
- checks if the correlations violate a **steering inequality**



Advantages:

✓ No trust in Alice required

✓ Less strong, but useful for one-sided secure QKD

✓ Robust to detection loophole

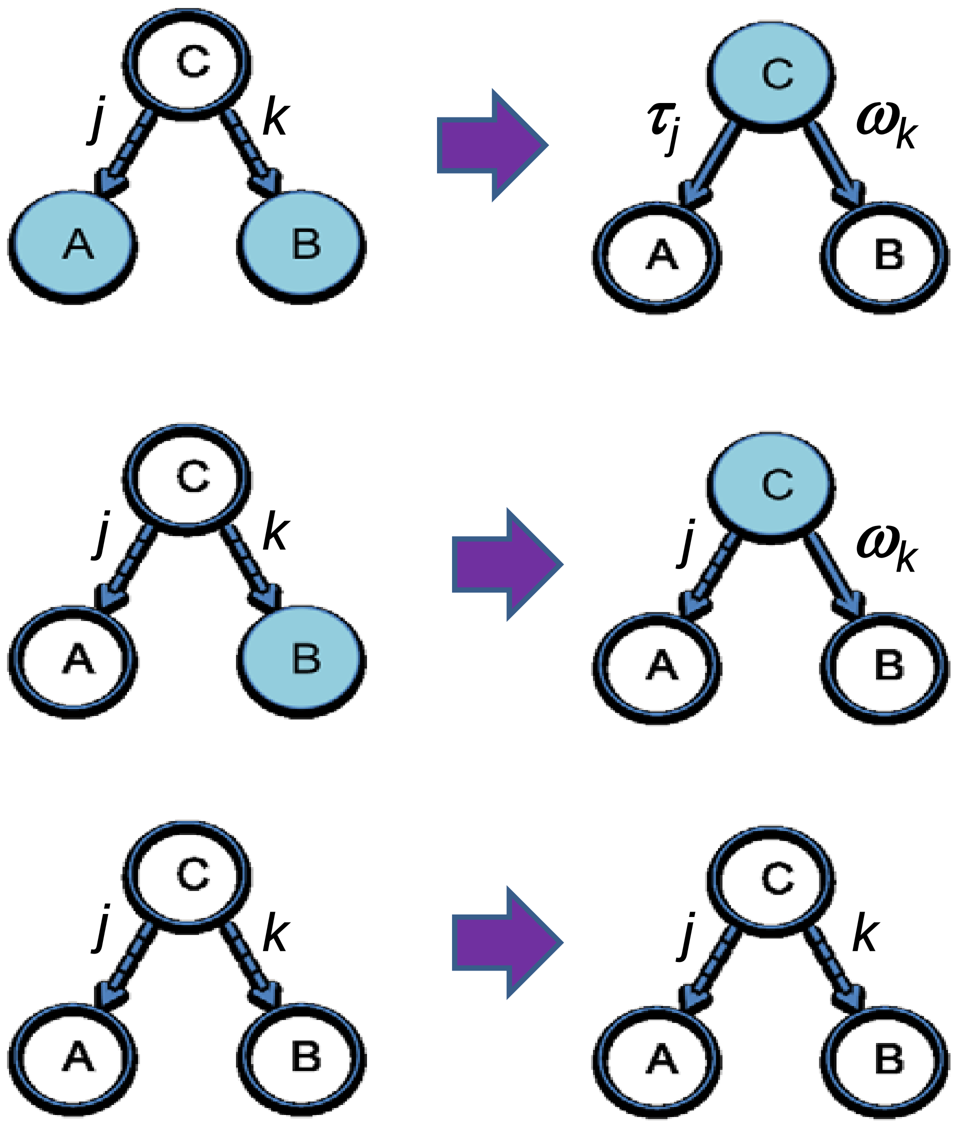
Disadvantage:

❖ Have to trust Bob and his devices

❖ **Out of date ?**

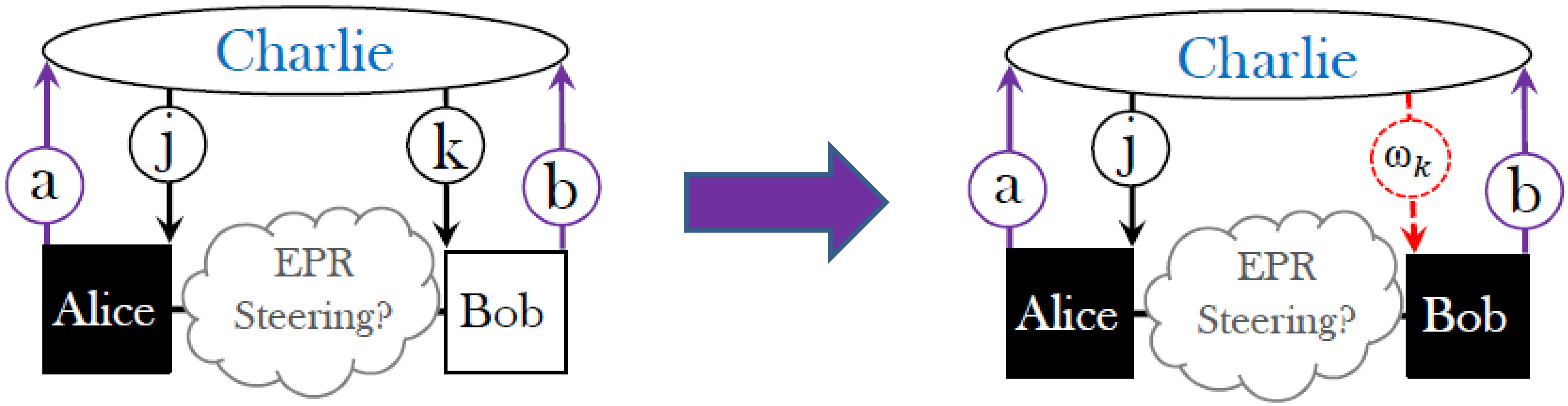
A new picture – no trust required!

(Buscemi, PRL **108** 200401, 2012; Cavalcanti et al, PRA **87** 032306, 2013)



- Replace trust in Alice and/or Bob by encoding *s* and/or *t* in quantum states
- Charlie need only trust QM, i.e., that Alice and Bob cannot discriminate between nonorthogonal quantum states
- <u>Quantum</u>-refereed games (⇒ measurement device independence)

Applying the new-fangled approach:
Quantum-refereed steering games



The old way: trust Bob

The new way: trust nobody!

- ✓ Trust in Bob is replaced by quantum input states, $\{\omega_k\}$
- ✓ Bob cannot cheat because he cannot distinguish them
- ✓ Still robust to detection loophole!

How to play the game?

- ✓ **Existence:** Cavalcanti *et al.,* PRA 87, 032306, 2013
  (building on Buscemi, PRL, 108, 200401, 2012)
- ✓ **Construction:** Kocsis *et al., Nature Commun.* 6, 6886, 2015
  (building on Branciard *et al.* PRL **110** 060405, 2013)

EXAMPLE OF A QUANTUM-REFEREED STEERING GAME

Charlie:

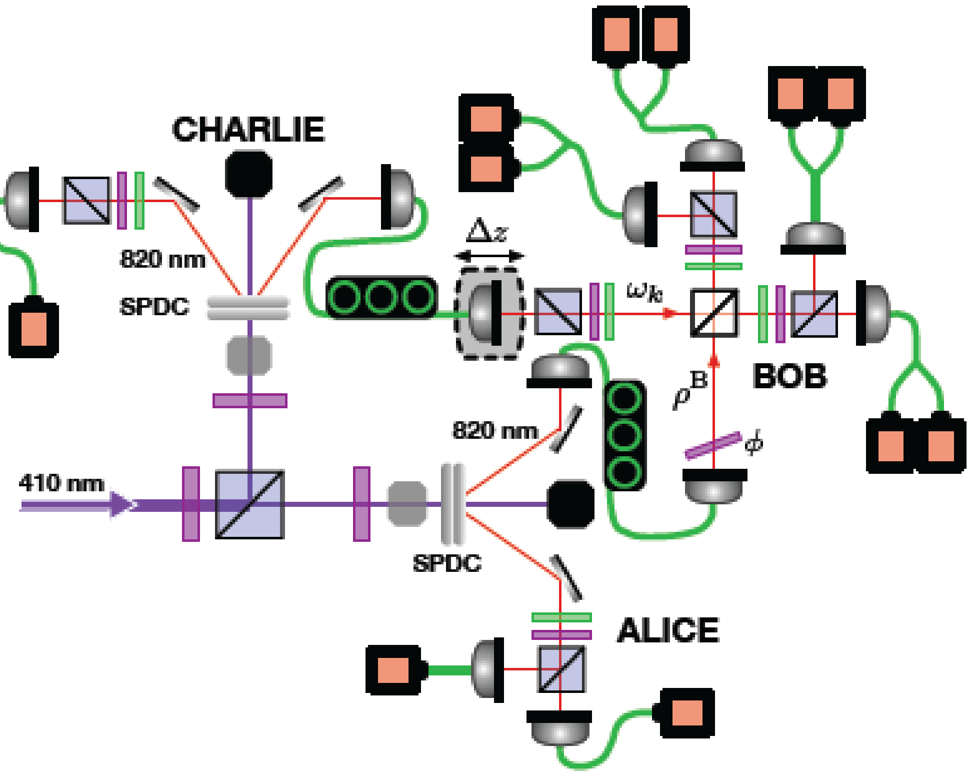
- sends input **j**=1,2,3 to Alice; receives output **a** = 1 or -1
- sends qubit input $\omega_j^{\pm} = \frac{1}{2}(1 \pm \sigma_j)$ to Bob; receives **b**=0 or 1.
- calculates the "payoff function"

$$P := 2 \sum_{j,s} \left[s \langle \mathbf{ab} \rangle - r \langle \mathbf{b} \rangle / \sqrt{3} \right]_{j,s} \qquad (r \geq 1)$$

P > 0 <u>guarantees</u> that Alice can steer Bob's state

Experiment: polarisation-encoded qubits

- Alice and Bob share a Werner state, comprising fractions
  W : singlet state,
  $1\text{-}W$: maximally-mixed state.
- Alice measures σ_j : **a**=1 or -1.
- Bob makes *projective Bell-state measurement* onto the singlet state **b**=0 or 1.



Payoff function:

$$P = 3W - \sqrt{3}$$

if Charlie prepares $\omega_j^{\pm}$ perfectly.

$\therefore$ need $W > 1/\sqrt{3}$ ~ 0.577, for P>0.

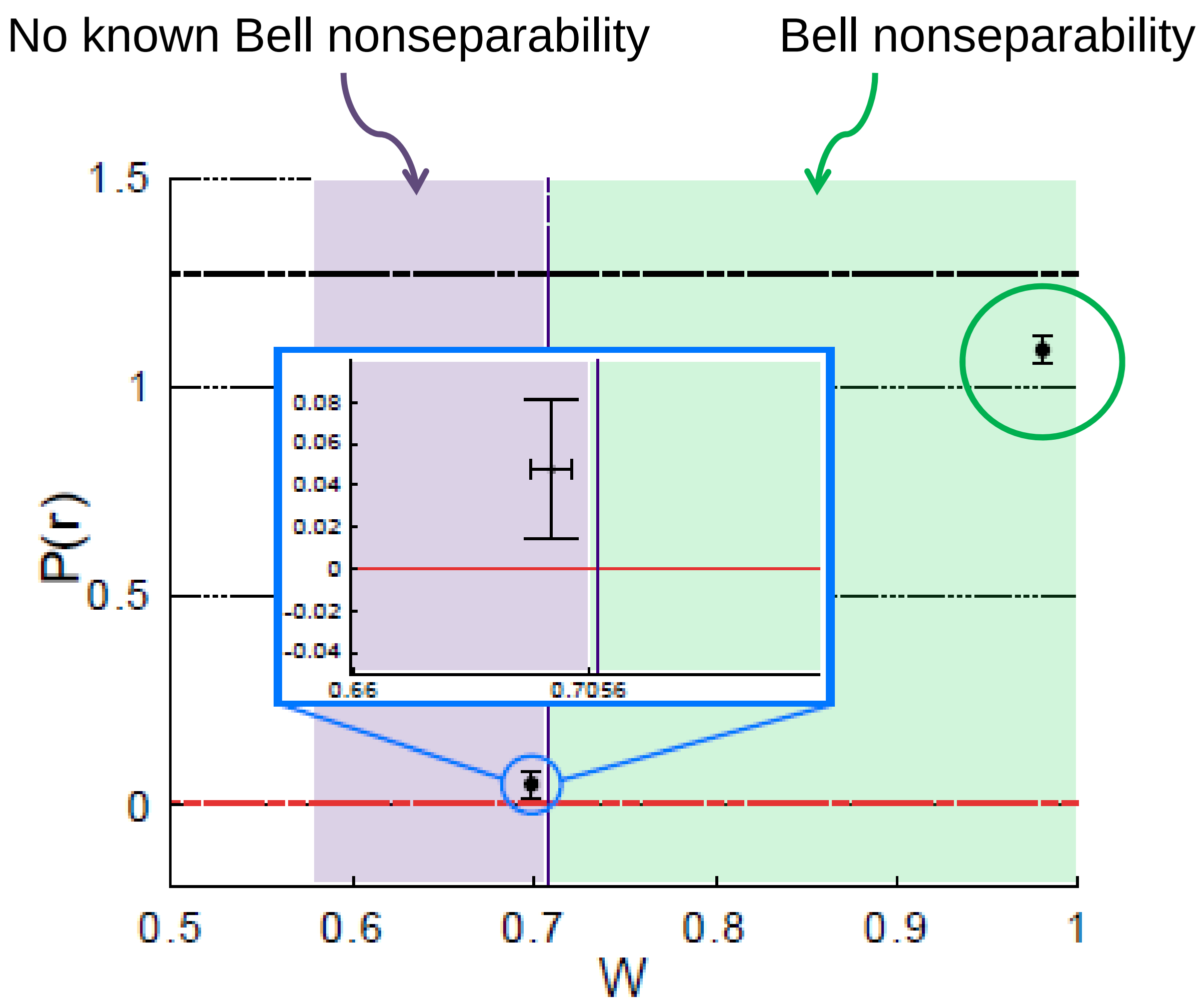
Modified payoff function:

$$P(r) = 3W - \sqrt{3}\,r \qquad (r \geq 1)$$

for imperfect preparation.

(r=1.081 for our experiment)

Experimental trust-free verification of steerability



Conclusions

Quantum-refereed steering games:

- allow verification of steering entanglement, without trust in either party or their devices – Charlie “quantum programs” them

- are robust to the detection loophole

- have been implemented in a proof-of-principle experiment, both with and without Bell nonseparability present

- hope to incorporate them into quantum communication protocols

THANK YOU !

Quantum-refereed games

For entanglement:

- Existence:
  - Buscemi 2012 (“semiquantum games”)
- Construction:
  - Branciard *et al.* PRL **110** 060405 (2013) (“measurement-device-independent entanglement witnesses”)
  - Rosset *et al.* NJP **15** 053025 (2013) (*with communication allowed*!)
- Experiment:
  - Xu *et al.* PRL **112** 140506 (2014)

For steering

- Existence:
  - Cavalcanti et al. 2013 (“quantum-refereed games”)
- Construction:
  - Kocsis *et al.*

    (“quantum-refereed steering games”)
- Experiment:
  - Kocsis *et al*. 2015