Universal Bell Correlations Do Not Exist

William M. Hoza[1]   Cole A. Graham[2]

December 4, 2016

CS395T – Quantum Complexity Theory

[1]Department of Computer Science, UT Austin

[2]Department of Mathematics, Stanford University

Quantum nonlocality

- Recall Bell's theorem: Entanglement allows interactions that can't be simulated using shared randomness / hidden variables

Quantum nonlocality

- Recall Bell's theorem: Entanglement allows interactions that can't be simulated using shared randomness / hidden variables
- Recall the no-communication theorem: Entanglement can't be used to send signals

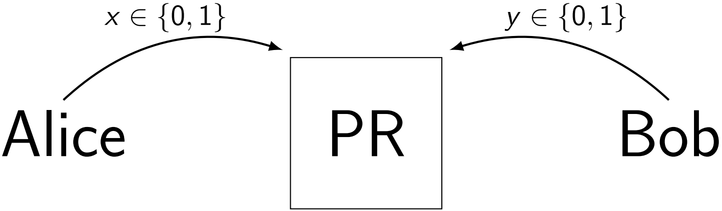
Quantum nonlocality

- Recall Bell's theorem: Entanglement allows interactions that can't be simulated using shared randomness / hidden variables
- Recall the no-communication theorem: Entanglement can't be used to send signals
- Contradictory?

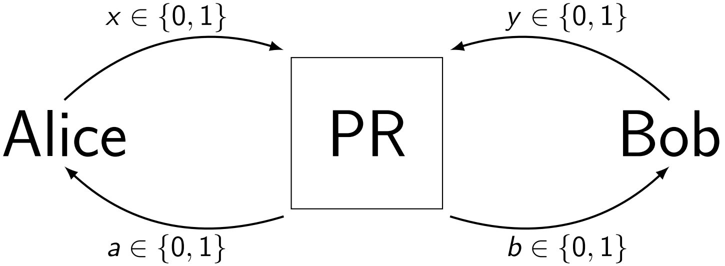
PR box

Alice $\boxed{\text{PR}}$ Bob

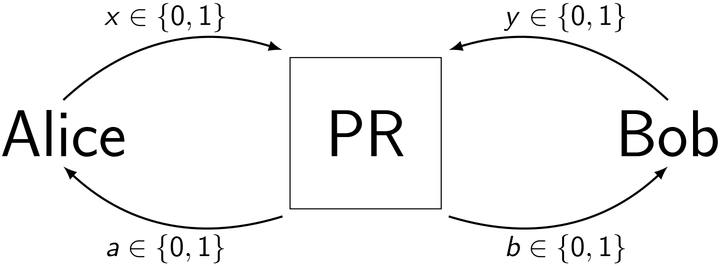
PR box



PR box

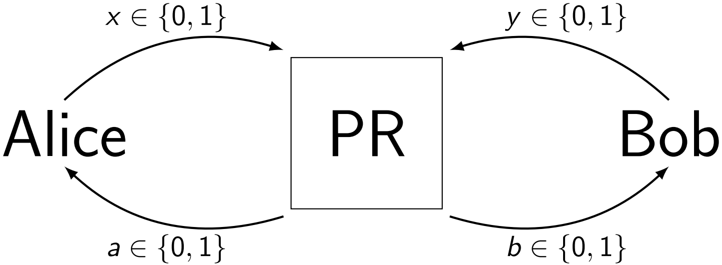


PR box



$$(a,b) = \begin{cases} (0, xy) & \text{with probability } 1/2 \\ (1, 1-xy) & \text{with probability } 1/2 \end{cases}$$

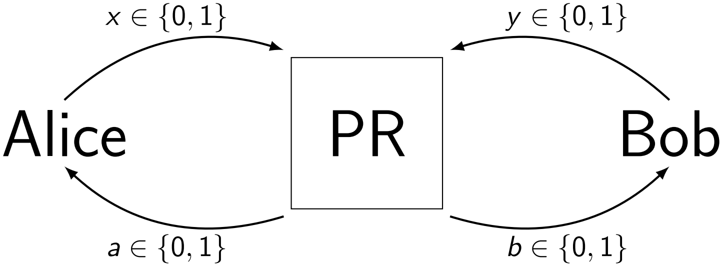
PR box



$$(a, b) = \begin{cases} (0, xy) & \text{with probability } 1/2 \\ (1, 1 - xy) & \text{with probability } 1/2 \end{cases}$$

- Cannot be used to communicate

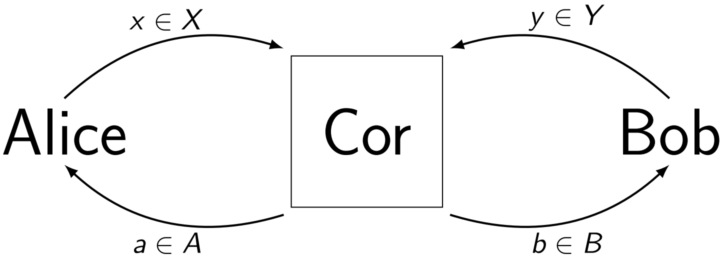
PR box



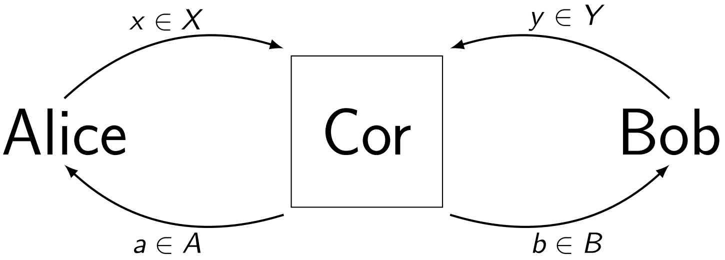
$$(a, b) = \begin{cases} (0, xy) & \text{with probability } 1/2 \\ (1, 1 - xy) & \text{with probability } 1/2 \end{cases}$$

- Cannot be used to communicate
- But can be used to win CHSH game: $a + b = xy \pmod 2$

Correlation box



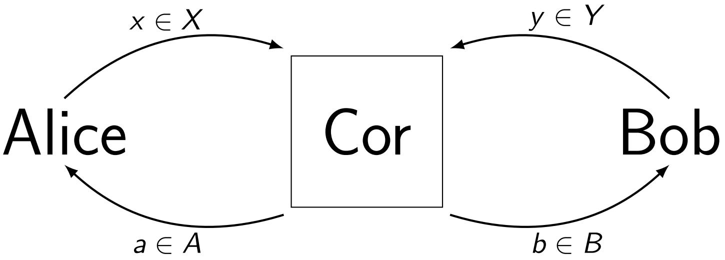
Correlation box



- A *correlation box* is a map

  $$\mathrm{Cor} : X \times Y \to \{\mu : \mu \text{ is a probability distribution over } A \times B\}$$

Correlation box

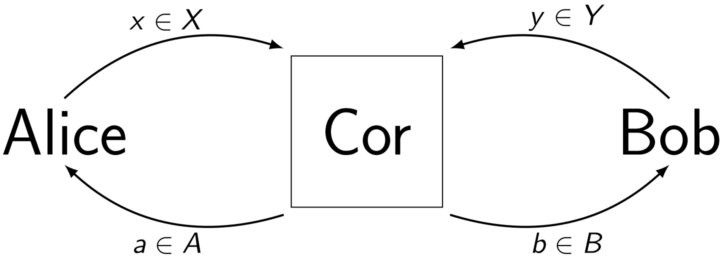


- A *correlation box* is a map

  $$\text{Cor} : X \times Y \to \{\mu : \mu \text{ is a probability distribution over } A \times B\}$$

- Assume X, Y, A, B are countable

Correlation box



- A *correlation box* is a map

  $$\mathrm{Cor} : X \times Y \to \{\mu : \mu \text{ is a probability distribution over } A \times B\}$$

- Assume X, Y, A, B are countable
- Abuse notation and write $\mathrm{Cor} : X \times Y \to A \times B$

Distributed sampling problems

$$
\begin{tikzcd}
 & \text{Referee} \arrow[dl, "x \in X"'] \arrow[dr, "y \in Y"] & \\
\text{Alice} \arrow[ur, "a \in A"'] & & \text{Bob} \arrow[ul, "b \in B"]
\end{tikzcd}
$$

- Can think of a correlation box as a *distributed sampling problem* – the problem of simulating the box

Distributed sampling complexity classes

- **SR**: class of correlation boxes that can be simulated using just shared randomness

Distributed sampling complexity classes

- **SR**: class of correlation boxes that can be simulated using just shared randomness
- **Q**: class of correlation boxes that can be simulated using shared randomness + arbitrary bipartite quantum state

Distributed sampling complexity classes

- **SR**: class of correlation boxes that can be simulated using just shared randomness
- **Q**: class of correlation boxes that can be simulated using shared randomness + arbitrary bipartite quantum state
- Obviously $\mathbf{SR} \subseteq \mathbf{Q}$

Distributed sampling complexity classes

- **SR**: class of correlation boxes that can be simulated using just shared randomness
- **Q**: class of correlation boxes that can be simulated using shared randomness + arbitrary bipartite quantum state
- Obviously $\mathbf{SR} \subseteq \mathbf{Q}$
- Bell's theorem: $\mathbf{SR} \neq \mathbf{Q}$

Distributed sampling complexity classes (2)

- **NS**: class of non-signalling correlation boxes

Distributed sampling complexity classes (2)

- **NS**: class of non-signalling correlation boxes
- No-communication theorem: $\mathbf{Q} \subseteq \mathbf{NS}$

Distributed sampling complexity classes (2)

- **NS**: class of non-signalling correlation boxes
- No-communication theorem: $\mathbf{Q} \subseteq \mathbf{NS}$
- Tsierelson bound: $\mathrm{PR} \notin \mathbf{Q}$, so $\mathbf{Q} \neq \mathbf{NS}$

Bell pair

- Goal: Understand $\mathbf{Q}$

Bell pair

- Goal: Understand **Q**
- Baby step: Understand **BELL**: class of correlation boxes that can be simulated using shared randomness + $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ + projective measurements

Bell pair

- Goal: Understand **Q**
- Baby step: Understand **BELL**: class of correlation boxes that can be simulated using shared randomness + $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ + projective measurements
- **SR** $\subsetneq$ **BELL** $\subsetneq$ **Q**

Toner-Bacon theorem

- Theorem (Toner, Bacon '03): **BELL** can be simulated using shared randomness + 1 bit of communication

Toner-Bacon theorem

- Theorem (Toner, Bacon '03): **BELL** can be simulated using shared randomness + 1 bit of communication
- This is an upper bound on the power of **BELL**

Toner-Bacon theorem

- Theorem (Toner, Bacon '03): **BELL** can be simulated using shared randomness + 1 bit of communication
- This is an upper bound on the power of **BELL**
- Loose upper bound, since **BELL** $\subseteq$ **NS**

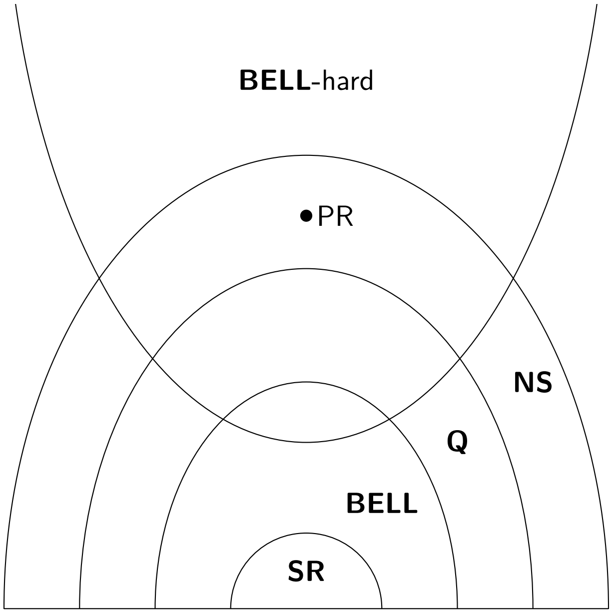
PR box is **BELL**-hard

- Theorem (Cerf et al. '05): **BELL** can be simulated using shared randomness + 1 PR box

PR box is **BELL**-hard

- Theorem (Cerf et al. '05): **BELL** can be simulated using shared randomness + 1 PR box
- In other words, PR is **BELL**-hard with respect to 1-query reductions

Distributed sampling complexity zoo



- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box

- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box
- ☹

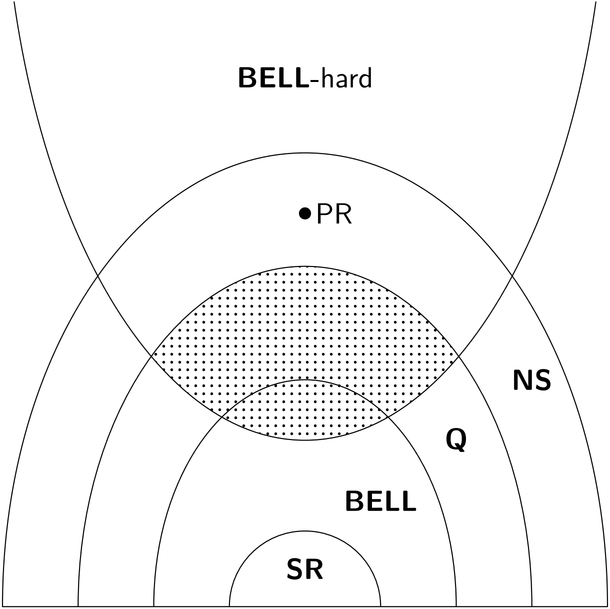
- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box
- ☹
- Theorem:

- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box
- ☹
- Theorem:
  - Suppose $\mathrm{Cor} : X \times Y \to A \times B$ is in **Q**; X, Y countable; A, B finite

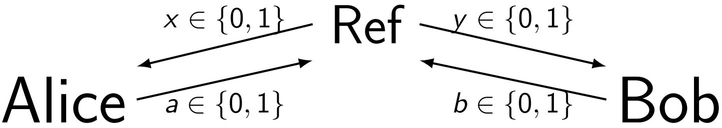
- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box
- ☹
- Theorem:
  - Suppose $\mathrm{Cor} : X \times Y \to A \times B$ is in **Q**; X, Y countable; A, B finite
  - Then there exists a binary correlation box in **BELL** that does not reduce to Cor

- Theorem: There does not exist a finite-alphabet **BELL**-complete correlation box
- ☹
- Theorem:
  - Suppose $\mathrm{Cor} : X \times Y \to A \times B$ is in **Q**; X, Y countable; A, B finite
  - Then there exists a binary correlation box in **BELL** that does not reduce to Cor
- ☹☹☹

Distributed sampling complexity zoo (2)

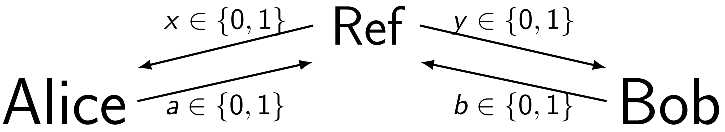


Biased CHSH game



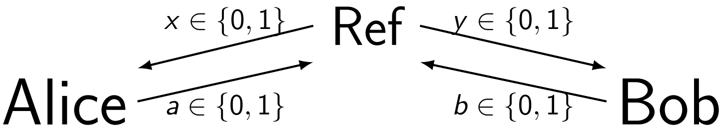
- Goal: $a + b = xy \pmod 2$

Biased CHSH game



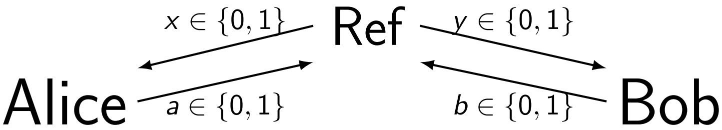
- Goal: $a + b = xy \pmod 2$
- Inputs x, y are chosen independently at random

Biased CHSH game



- Goal: $a + b = xy \pmod 2$
- Inputs x, y are chosen independently at random
- y is uniform, x is biased: $\Pr[x = 1] = p \in [1/2, 1]$

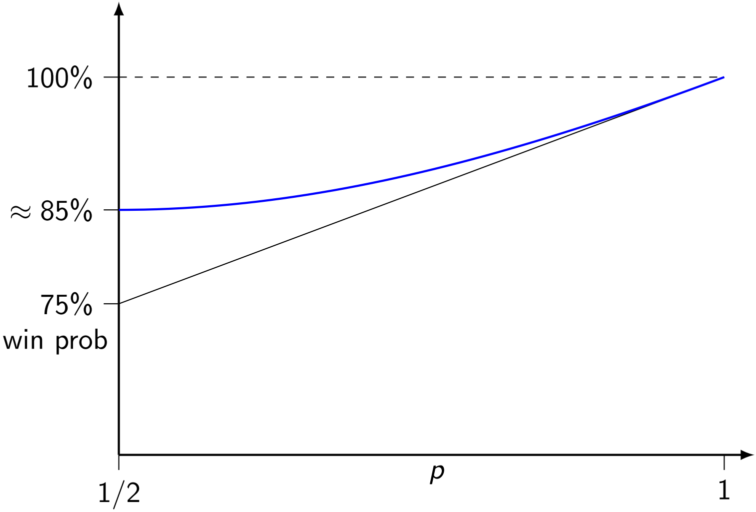
Biased CHSH game



- Goal: $a + b = xy \pmod 2$
- Inputs x, y are chosen independently at random
- y is uniform, x is biased: $\Pr[x = 1] = p \in [1/2, 1]$
- Theorem (Lawson, Linden, Popescu '10): Optimal quantum strategy can be implemented in **BELL**, wins with probability

$$f(p) \stackrel{\text{def}}{=} \frac{1}{2} + \frac{1}{2}\sqrt{p^2 + (1-p)^2}$$

Quantum value of biased CHSH game



Affine functions from reductions

- Let $S_p \in \textbf{BELL}$ be optimal quantum strategy

Affine functions from reductions

- Let $\mathsf{S}_p \in \mathbf{BELL}$ be optimal quantum strategy
- Assume there is a reduction from S_p to Cor

Affine functions from reductions

- Let $\mathsf{S}_p \in \mathbf{BELL}$ be optimal quantum strategy
- Assume there is a reduction from S_p to Cor
- Probability that reduction wins biased CHSH game is of form

$$\frac{1-p}{2}P_{00} + \frac{p}{2}P_{10} + \frac{1-p}{2}P_{01} + \frac{p}{2}P_{11}$$

Affine functions from reductions

- Let $S_p \in \mathbf{BELL}$ be optimal quantum strategy
- Assume there is a reduction from S_p to Cor
- Probability that reduction wins biased CHSH game is of form

$$\frac{1-p}{2} P_{00} + \frac{p}{2} P_{10} + \frac{1-p}{2} P_{01} + \frac{p}{2} P_{11}$$

- Affine function of p, for fixed reduction

Countably many affine functions

- Fix shared randomness without decreasing win probability

Countably many affine functions

- Fix shared randomness without decreasing win probability
- Recall Cor $\in \mathbf{Q}$

Countably many affine functions

- Fix shared randomness without decreasing win probability
- Recall Cor $\in \mathbf{Q}$
- Win probability still exactly $f(p)$ ($\mathbf{Q}$ is closed under reductions)

Countably many affine functions

- Fix shared randomness without decreasing win probability
- Recall $\mathrm{Cor} \in \mathbf{Q}$
- Win probability still exactly $f(p)$ ($\mathbf{Q}$ is closed under reductions)
- Recall $\mathrm{Cor} : X \times Y \to A \times B$ with X, Y countable, A, B finite

Countably many affine functions

- Fix shared randomness without decreasing win probability
- Recall Cor $\in \mathbf{Q}$
- Win probability still exactly $f(p)$ ($\mathbf{Q}$ is closed under reductions)
- Recall $\mathrm{Cor} : X \times Y \to A \times B$ with X, Y countable, A, B finite
- Only countably many deterministic reductions!

Countably many affine functions

- Fix shared randomness without decreasing win probability
- Recall Cor $\in \mathbf{Q}$
- Win probability still exactly $f(p)$ ($\mathbf{Q}$ is closed under reductions)
- Recall Cor : $X \times Y \to A \times B$ with X, Y countable, A, B finite
- Only countably many deterministic reductions!
- Countably many affine functions, so $\exists p$ where all the affine functions disagree with $f(p)$

Approximate simulations

- Theorem:

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in \mathbf{BELL}$ such that

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in$ **BELL** such that
  - If there is a k-query ε-error reduction from Cor_1 to Cor_2, then

$$k^4 \cdot (2|X|)^{2|A|^k} \cdot (2|Y|)^{2|B|^k} \geq \Omega(1/\varepsilon)$$

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in$ **BELL** such that
  - If there is a k-query ε-error reduction from Cor_1 to Cor_2, then

$$k^4 \cdot (2|X|)^{2|A|^k} \cdot (2|Y|)^{2|B|^k} \geq \Omega(1/\varepsilon)$$

- Upper bound: $\forall \varepsilon > 0, \exists \mathrm{Cor}_2 : [T] \times [T] \to \{0,1\} \times \{0,1\}$ such that

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in \mathbf{BELL}$ such that
  - If there is a k-query ε-error reduction from Cor_1 to Cor_2, then

$$k^4 \cdot (2|X|)^{2|A|^k} \cdot (2|Y|)^{2|B|^k} \geq \Omega(1/\varepsilon)$$

- Upper bound: $\forall \varepsilon > 0, \exists \mathrm{Cor}_2 : [T] \times [T] \to \{0,1\} \times \{0,1\}$ such that
  - $T \leq O(1/\varepsilon^4)$

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in$ **BELL** such that
  - If there is a k-query ε-error reduction from Cor_1 to Cor_2, then

$$k^4 \cdot (2|X|)^{2|A|^k} \cdot (2|Y|)^{2|B|^k} \geq \Omega(1/\varepsilon)$$

- Upper bound: $\forall \varepsilon > 0, \exists \mathrm{Cor}_2 : [T] \times [T] \to \{0,1\} \times \{0,1\}$ such that
  - $T \leq O(1/\varepsilon^4)$
  - $\mathrm{Cor}_2 \in$ **BELL**

Approximate simulations

- Theorem:
  - Suppose $\mathrm{Cor}_2 : X \times Y \to A \times B$ is in $\mathbf{Q}$; X, Y, A, B finite
  - Then $\exists$ binary correlation box $\mathrm{Cor}_1 \in \mathbf{BELL}$ such that
  - If there is a k-query ε-error reduction from Cor_1 to Cor_2, then

$$k^4 \cdot (2|X|)^{2|A|^k} \cdot (2|Y|)^{2|B|^k} \geq \Omega(1/\varepsilon)$$

- Upper bound: $\forall \varepsilon > 0, \exists \mathrm{Cor}_2 : [T] \times [T] \to \{0,1\} \times \{0,1\}$ such that
  - $T \leq O(1/\varepsilon^4)$
  - $\mathrm{Cor}_2 \in \mathbf{BELL}$
  - For every $\mathrm{Cor}_1 \in \mathbf{BELL}$, there is a 1-query ε-error reduction from Cor_1 to Cor_2

Conclusions

- Is there a countable-alphabet **BELL**-complete correlation box?

Conclusions

- Is there a countable-alphabet **BELL**-complete correlation box?
- What is the right relationship between $|X|, |Y|, |A|, |B|, k, \varepsilon$?

Conclusions

- Is there a countable-alphabet **BELL**-complete correlation box?
- What is the right relationship between $|X|, |Y|, |A|, |B|, k, \varepsilon$?
- Thanks for listening! Questions?
- This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No. DGE-1610403.
- Cole Graham gratefully acknowledges the support of the Fannie and John Hertz Foundation.