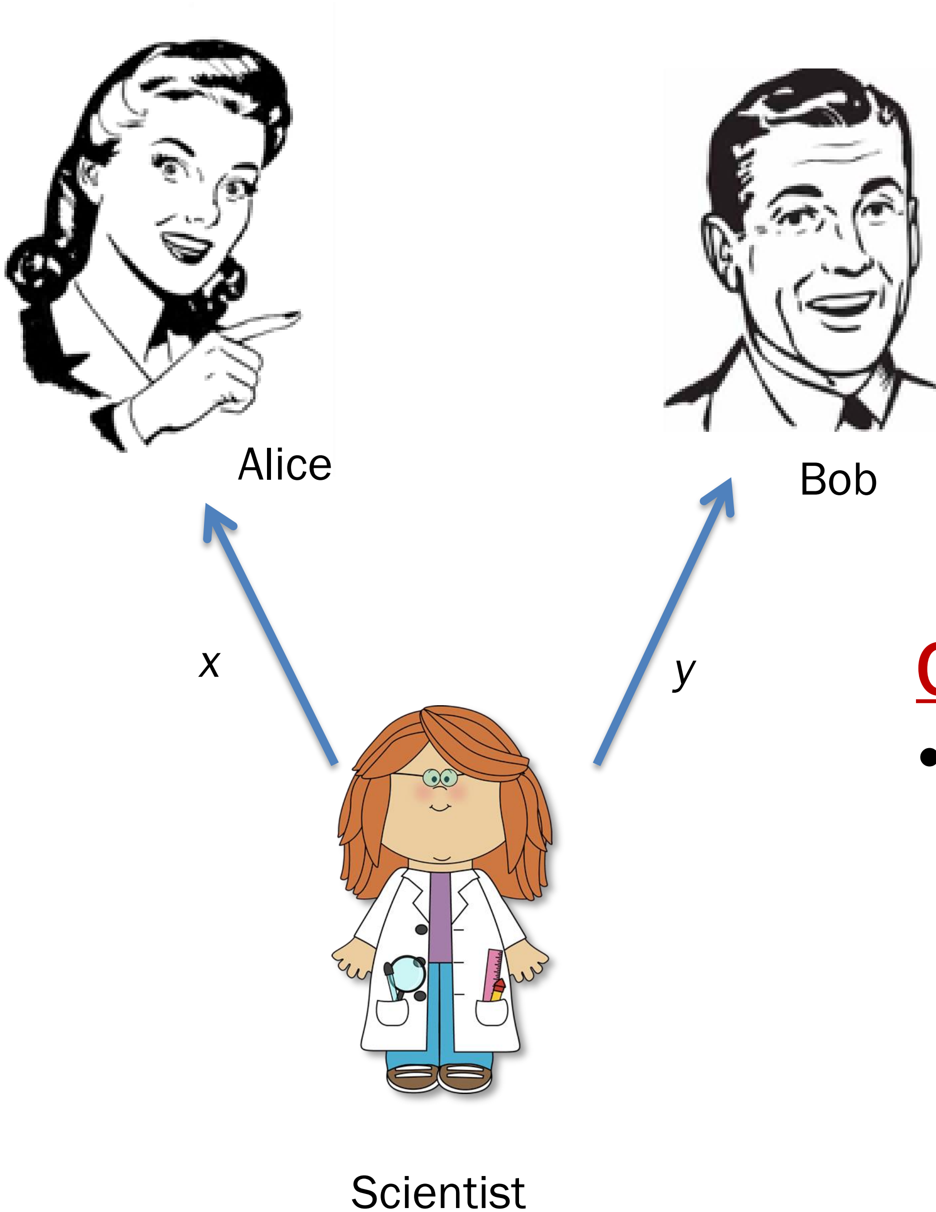
# A parallel repetition theorem for *all* entangled games


Henry Yuen

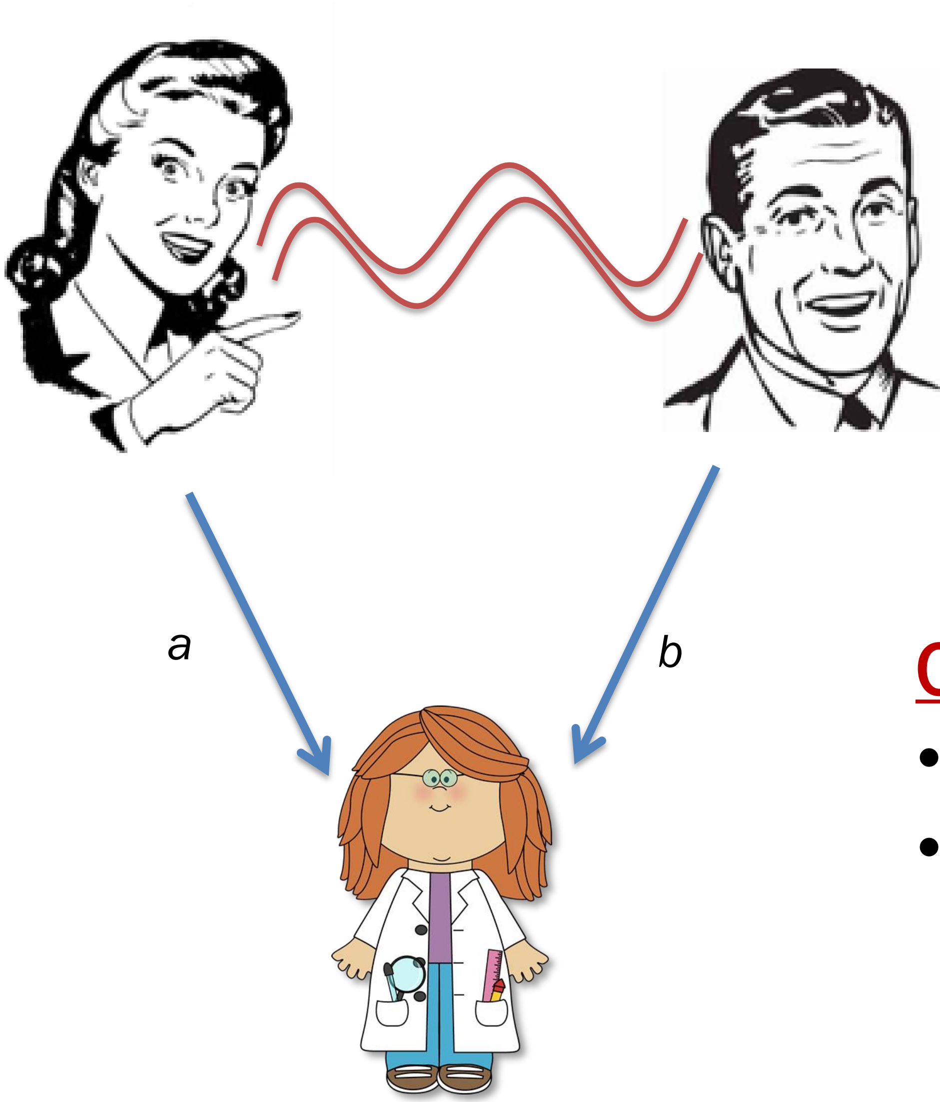
*UC Berkeley*


*QIP 2017*
*Seattle, WA*




## CHSH game

- $x$, $y$ uniform bits

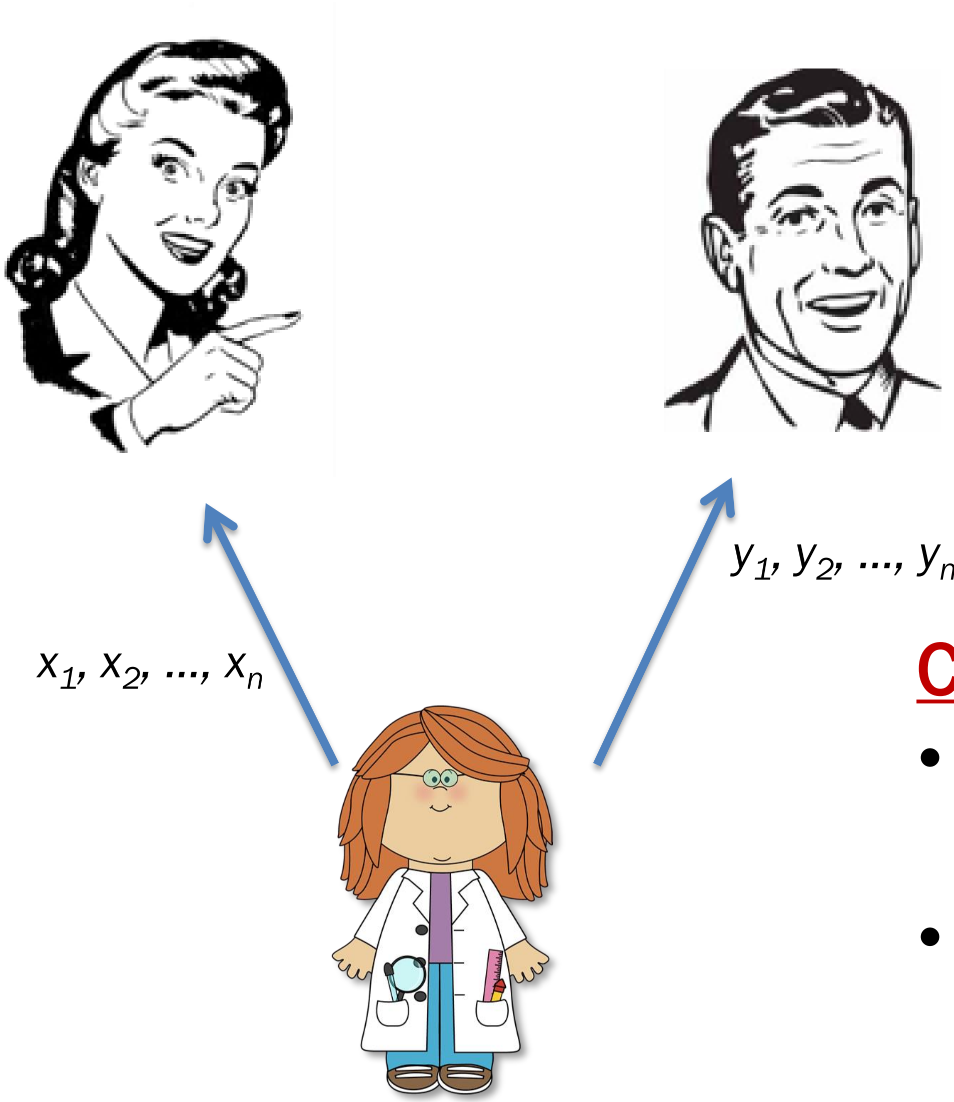



**Bell's theorem:**
val*(CHSH) > val(CHSH)

## CHSH game

- $x$, $y$ uniform bits
- Players win if
  $a \oplus b = x \wedge y$.

Max classical win prob: val(CHSH) = 3/4
Max quantum win prob: val*(CHSH) = $\cos^2(\pi/8) \approx .854...$




## CHSH$^n$ game

- $x_1,\ldots,x_n$
  $y_1,\ldots,y_n$ uniform bits
- Win iff $a_i \oplus b_i = x_i \wedge y_i$ *for all* i.

What is val(CHSH$^n$)? What about val*(CHSH$^n$)

# Easy observation:

1. $\text{val}(\text{CHSH}^n) \geq \text{val}(\text{CHSH})^n = (3/4)^n$

2. $\text{val}^*(\text{CHSH}^n) \geq \text{val}^*(\text{CHSH})^n = (.854...)^n$

# Proof:

The players can simply play each round independently!

# Exactly one of these is true:

1. val(CHSH$^n$) = val(CHSH)$^n$ = (3/4)$^n$ ✗

   Ambainis 2014:

$$\lim_{n\to\infty} \sqrt[n]{val(CHSH^n)} = \left(\frac{1+\sqrt{5}}{4}\right) = 0.809\ldots$$

2. val*(CHSH$^n$) = val*(CHSH)$^n$ = (.854...)$^n$ ✓

   Cleve, Slofstra, Unger, Upadhyay **2006:** Entangled value of XOR games satisfy *perfect parallel repetition*:

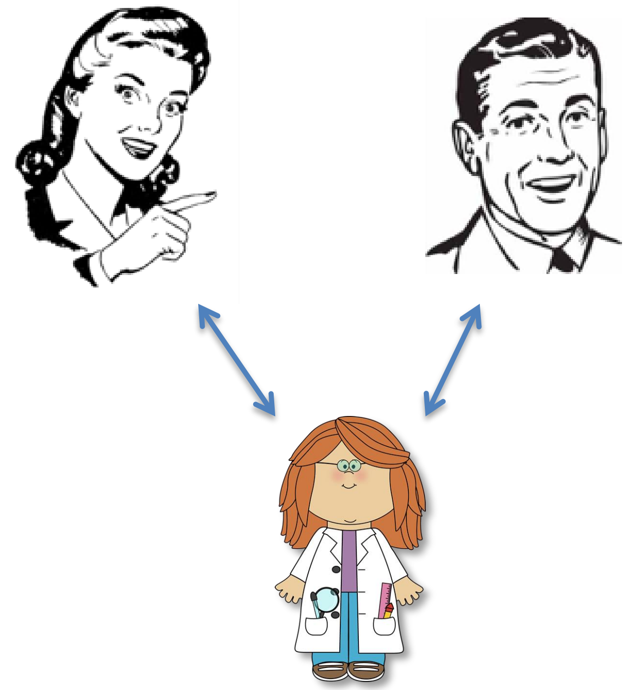
$$val^*(G^n) = val^*(G)^n$$

   Entangled value of XOR games has an SDP characterization, and the SDP *tensorizes* under parallel repetition.

# Parallel Repetition Question

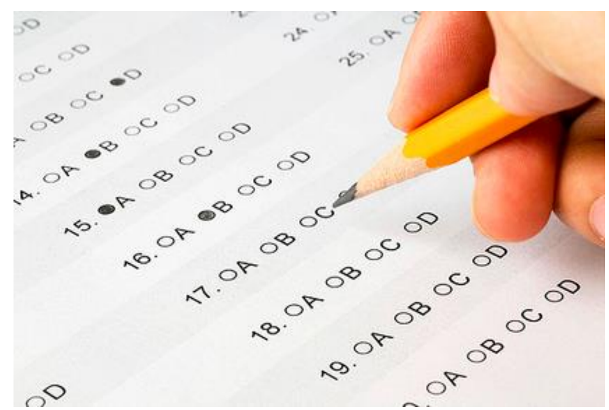
Two-player game G:

- question distribution $\pi(x,y)$
- verification predicate V(x,y,a,b)



1. val($G^n$) vs. val$(G)^n$?
2. val*($G^n$) vs. val*$(G)^n$ ?

# Parallel repetition is *weird*



**(Classical) Parallel Repetition Theorem** [Raz '95]

If val(G) = 1 – ε, then

$$\mathrm{val}(G^n) \leq \exp(-\Omega(\varepsilon^{32}\, n/s))$$

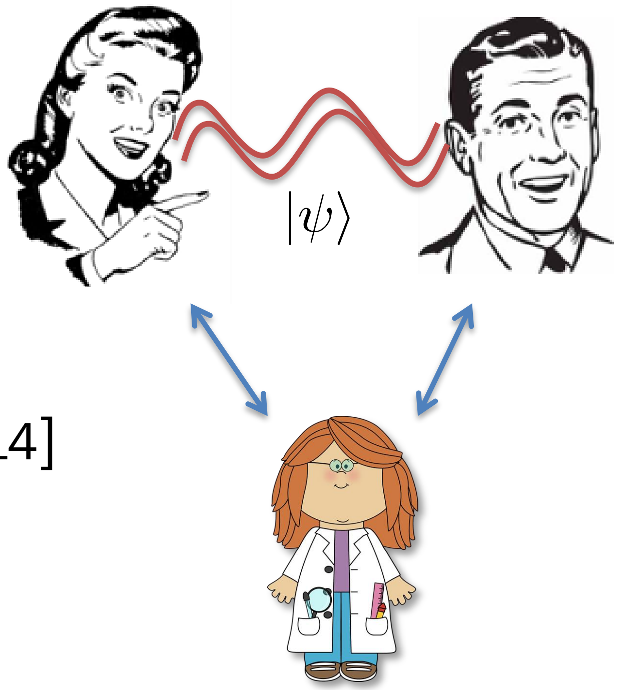
$s$ = length of players' answers.

- For nontrivial games G (val(G) < 1), the repeated game value goes to 0 exponentially fast.
- Influ
    - p
    - h
    - communication complexity
    - cryptography.
- Not an easy proof!

**What about the quantum case?**

# Quantum parallel repetition theorems

- XOR games [Cleve, Slofstra, Unger, Upadhyay 2006]
- Unique games [Kempe, Regev, Toner 2008]
- Feige-Kilian games [Kempe, Vidick 2011]
- Free games
  - Jain, Pereszlenyi, Yao 2014
  - Chailloux and Scarpa 2014
  - Chung, Wu, Y. 2015
- Projection games [Dinur, Steurer, Vidick 2014]
- Anchored games [Bavarian, Vidick. Y. 2015]
- Fortified games [Bavarian, Vidick. Y. 2016]




**But no proof of decay for general games!**

# Main Result

If **val*(G) = 1 – ε**, then

$$\text{val}^*(G^n) \leq O\left(\frac{s \log n}{\epsilon^{17}\, n^{1/4}}\right)$$

*s* = length of players' answers.

- As *n* goes to infinity, val*($G^n$) goes to 0.
- First decay bound for ***general*** entangled games.
- Quantum analogue of Verbitsky's theorem.

# Proof sketch

# Proof by contradiction

- Start by assuming there is a **supergood** strategy for $G^n$

State: $|\psi\rangle$

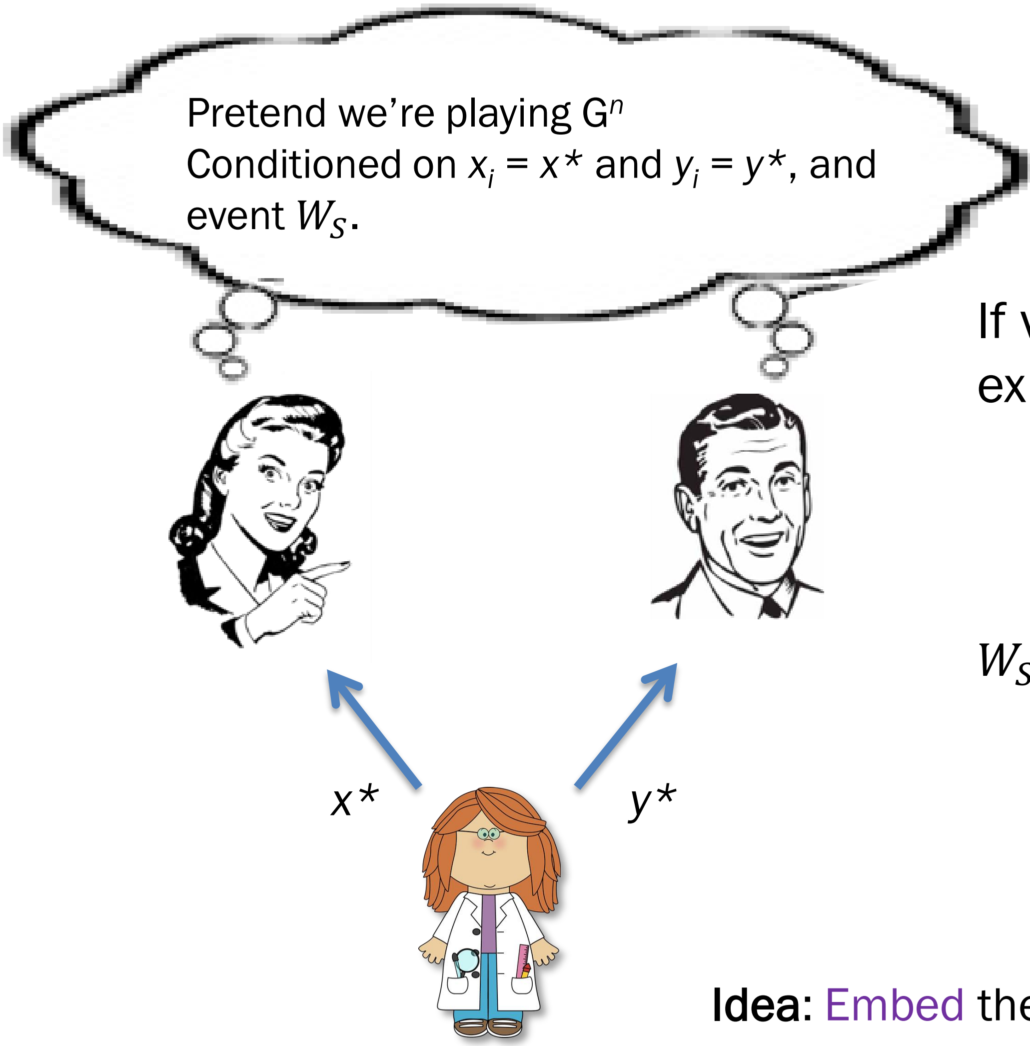
Measurements

Alice: $A_{x_1 \cdots x_n}(a_1 \ldots a_n)$

Bob: $B_{y_1 \cdots y_n}(b_1 \ldots b_n)$

$$p(\vec{a}, \vec{b} | \vec{x}, \vec{y}) = \langle \psi | A_{\vec{x}}(\vec{a}) \otimes B_{\vec{y}}(\vec{b}) | \psi \rangle$$

- **Assumption**: val*($G^n$) >> poly($s, n^{-1}, \varepsilon^{-1}$)
- **Goal**: obtain an entangled strategy for G with success probability greater than val*(G). **Contradiction.**




$$(x^*, y^*) \sim \pi$$

If $\mathrm{val}^*(G^n)$ too large, then there exists "nice" event $W_S$

$$\Pr(\text{ Win } i \mid W_S) > \mathrm{val}^*(G) + \delta$$

$W_S$: Winning in a set of rounds $S \subset [n]$

**Idea:** Embed the game G into the $i$'th round of $G^n$, conditioned on the event $W_S$, without communication.

# Conditioning entangled games

- Classically, embedding G into $G^n$ in the event $W_S$ requires careful conditioning of probability distributions.

- However, the notion of "conditioning" quantum entanglement is risky and dangerous.

- For all $(x^*,y^*)$, define an advice state

$$|\Phi_{x^* y^*}\rangle$$

representing $G^n$ conditioned on:

  - $i$'th inputs are $(x^*,y^*)$
  - Event $W_S$

# Strategy for G

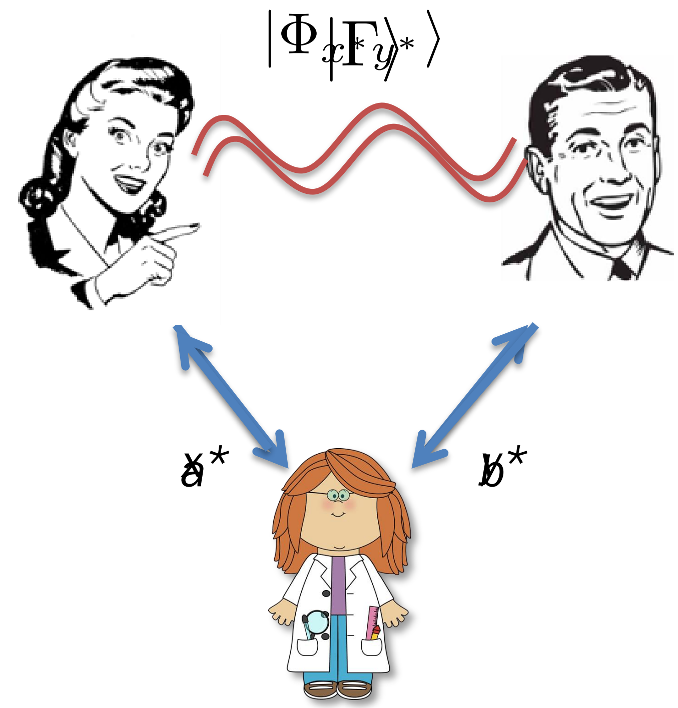
- Suppose the players, upon receiving *x** and *y**, can generate $|\Phi_{x^*y^*}\rangle$ using preshared entanglement and local operations.

- By measuring, players get answers (*a*,*b*) satisfying V(*x**,*y**,*a*,*b*) = 1 with prob.

  $$\Pr(\text{ Win } i \mid W_S, x^*, y^*)$$

- On average over (*x**,*y**) ~ μ, this is approximately

  $$\Pr(\text{ Win } i \mid W_S) > \text{val}^*(G) + \delta$$



**This would achieve the contradiction!**

# Sampling $|\Phi_{x^* y^*}\rangle$ without communication.

- This is the main challenge in proving parallel repetition theorems for entangled games.
- Problem: Alice does not know $y^*$ and Bob does not know $x^*$. Thus neither Alice nor Bob "knows" the full description of $|\Phi_{x^* y^*}\rangle$.
- Solution: show there exist local unitaries $U_{x^*}$ and $V_{y^*}$ such that

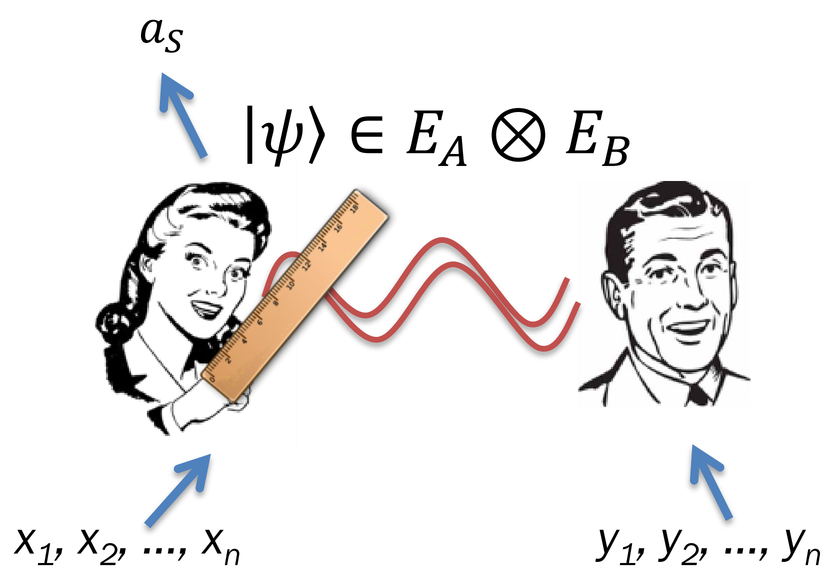
$$U_{x^*} \otimes V_{y^*} |\Phi_{x^* y^*}\rangle \approx |\Gamma\rangle$$

for some universal state $|\Gamma\rangle$.

# Defining and analyzing $|\Phi_{x^*y^*}\rangle$ in 3 easy steps.

Imagine Alice and Bob play $G^n$ using ***supergood*** strategy.

...but only ***Alice*** measures, and outputs answers in *S.*




**Step 1**:

$$I(X_i : E_B | A_S X_s)_\rho \le \frac{|S| \log|\Sigma_A|}{n}$$

for avg. coordinate $i \in [n] \setminus S$

Global state: $\rho^{XYA_SE_AE_B}$

1. X, Y, $A_S$ — classical
2. $E_AE_B$ — quantum post-measurement state

# Defining and analyzing $|\Phi_{x^* y^*}\rangle$ in 3 easy steps.

**Step 1 :**

$$I(X_i\!: E_B | A_S X_s)_\rho \leq \frac{|S| \log|\Sigma_A|}{n}$$

for avg. coordinate $i \in [n] \setminus S$

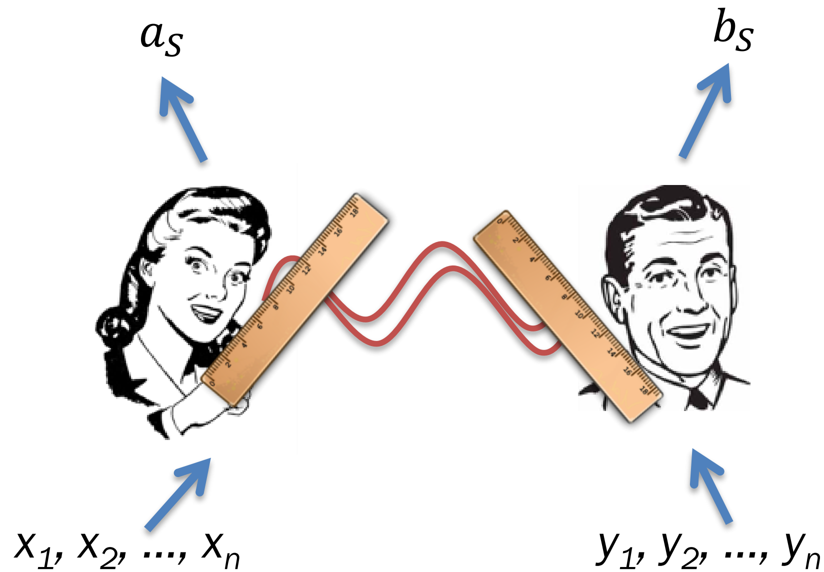
**Step 2:**

For every x there exists a purification $|\Delta_x\rangle \in E_A \otimes E_B$ of $\rho^{E_B}$ conditioned on

$A_S X_s$ and $X_i = x$

s.t for most $x, x'$,

$$|\Delta_x\rangle \approx_\delta |\Delta_{x'}\rangle$$




**Our advice state*:**

$$|\Phi_{x,y}\rangle \propto \sqrt{\mathbb{E} B^{b_S}_{y_1 \cdots y_n}} |\Delta_x\rangle$$

Expectation over all y's with $y_i = y$ and some fixing of $Y_S$.

# Defining and analyzing $|\Phi_{x^* y^*}\rangle$ in 3 easy steps.

**Step 1:**

$$I(X_i : E_B | A_S X_s)_\rho \le \frac{|S| \log|\Sigma_A|}{n}$$

for avg. coordinate $i \in [n] \setminus S$

**Step 2:**

For every x there exists a purification $|\Delta_x\rangle \in E_A \otimes E_B$ of $\rho^{E_B}$ conditioned on

$A_S X_s$ and $X_i = x$

s.t for most $x, x'$,

$$|\Delta_x\rangle \approx_\delta |\Delta_{x'}\rangle$$

**Our advice state*:**

$$|\Phi_{x,y}\rangle \propto \sqrt{\mathbb{E} B^{b_S}_{y_1 \cdots y_n}} |\Delta_x\rangle$$

Expectation over all y's with $y_i = y$ and some fixing of $Y_S$.

**Step 3:**

For most $x, x'$,

$$\| |\Phi_{x,y}\rangle - |\Phi_{x',y}\rangle \| \le \delta / \Pr(W_s)$$

**Step 3**:

For most $x, x', y$,

$$\left\| |\Phi_{x,y}\rangle - |\Phi_{x',y}\rangle \right\| \leq \delta / \Pr(W_s)$$

1. $\Pr(W_s) \geq \Pr(W)$
2. $\left\| |\Phi_{x,y}\rangle - |\Phi_{x',y}\rangle \right\| \leq \delta / \Pr(W) \leq \left( \frac{|S| \log|\Sigma_A|}{n} \right)^{1/4} \frac{1}{\Pr(W)}$
3. Since strategy was ***supergood***, this distance is at most $\sqrt{\delta}$.

**Step 3:**
For most $x, x', y, y'$,

$$\left\| |\Phi_{x,y}\rangle - |\Phi_{x',y}\rangle \right\| \leq \sqrt{\delta}$$

$$\left\| |\Phi_{x,y}\rangle - |\Phi_{x,y'}\rangle \right\| \leq \sqrt{\delta}$$

1. $\Pr(W_s) \geq \Pr(W)$
2. $\left\| |\Phi_{x,y}\rangle - |\Phi_{x',y}\rangle \right\| \leq {}^{\delta}/_{\Pr(W)} \leq \left(\frac{|S| \log|\Sigma_A|}{n}\right)^{1/4} \frac{1}{\Pr(W)}$
3. Since strategy was ***supergood***, this distance is at most $\sqrt{\delta}$.

**Quantum Correlated Sampling (Dinur, Steurer, Vidick 2014)**
Step 3 implies for most $x, y$, there exist local unitaries $U_x, V_y$ such that

$$U_x \otimes V_y |\Gamma\rangle \approx_{\delta^{1/6}} |\Phi_{x,y}\rangle \otimes |\gamma\rangle$$

where $|\Gamma\rangle, |\gamma\rangle$ are embezzlement states.

# Strategy for G

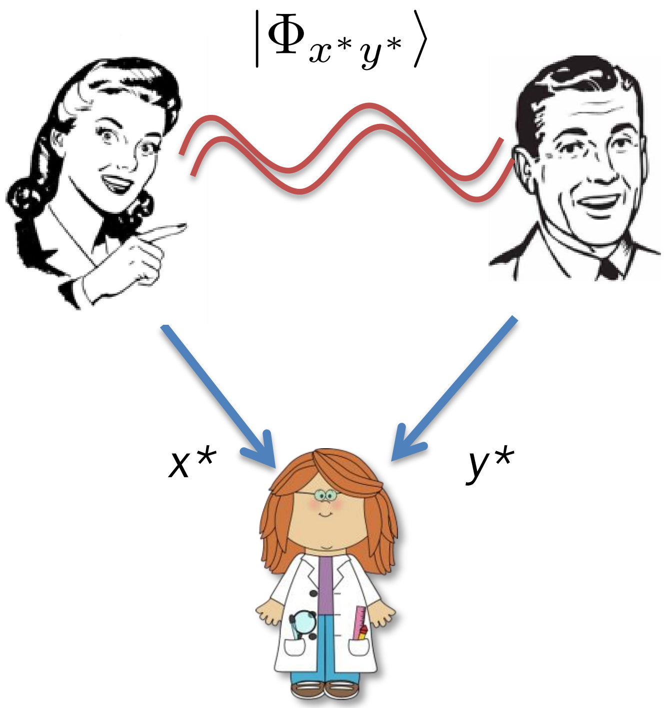
- Suppose the players, upon receiving *x** and *y**, can generate $|\Phi_{x^* y^*}\rangle$ using preshared entanglement and local operations.

- By measuring, players get answers (*a*,*b*) satisfying V(*x**,*y**,*a*,*b*) = 1 with prob.

  Pr( Win *i* | $W_S$, *x**, *y**)

- On average over (*x**,*y**) ~ μ, this is approximately

  Pr( Win *i* | $W_S$) > val*(G) + $\delta^{1/6}$




Contradiction!

# Summary and open questions

- **Main Result:** A quantum analogue of Raz's parallel repetition theorem holds with polynomial decay.

- If one is willing to tweak the game slightly, we can obtain exponential decay parallel repetition theorems for general games with entangled players. (joint work with Bavarian and Vidick)

- **Open questions**
  1. Quantum parallel repetition with exponential decay
  2. Classical parallel repetition of games with more than two players
  3. Direct product theorems for quantum communication complexity
  4. Is entanglement useful in the quantum communication complexity context?

## Thanks! Any questions?

If I don't get to your question, please ask Zhengfeng.