Embezzlement-based non-local game that cannot be played optimally with finite amount of entanglement

Rocky Mountain Summit on Quantum Information
June 28, 2018, JILA, University of Colorado, Boulder

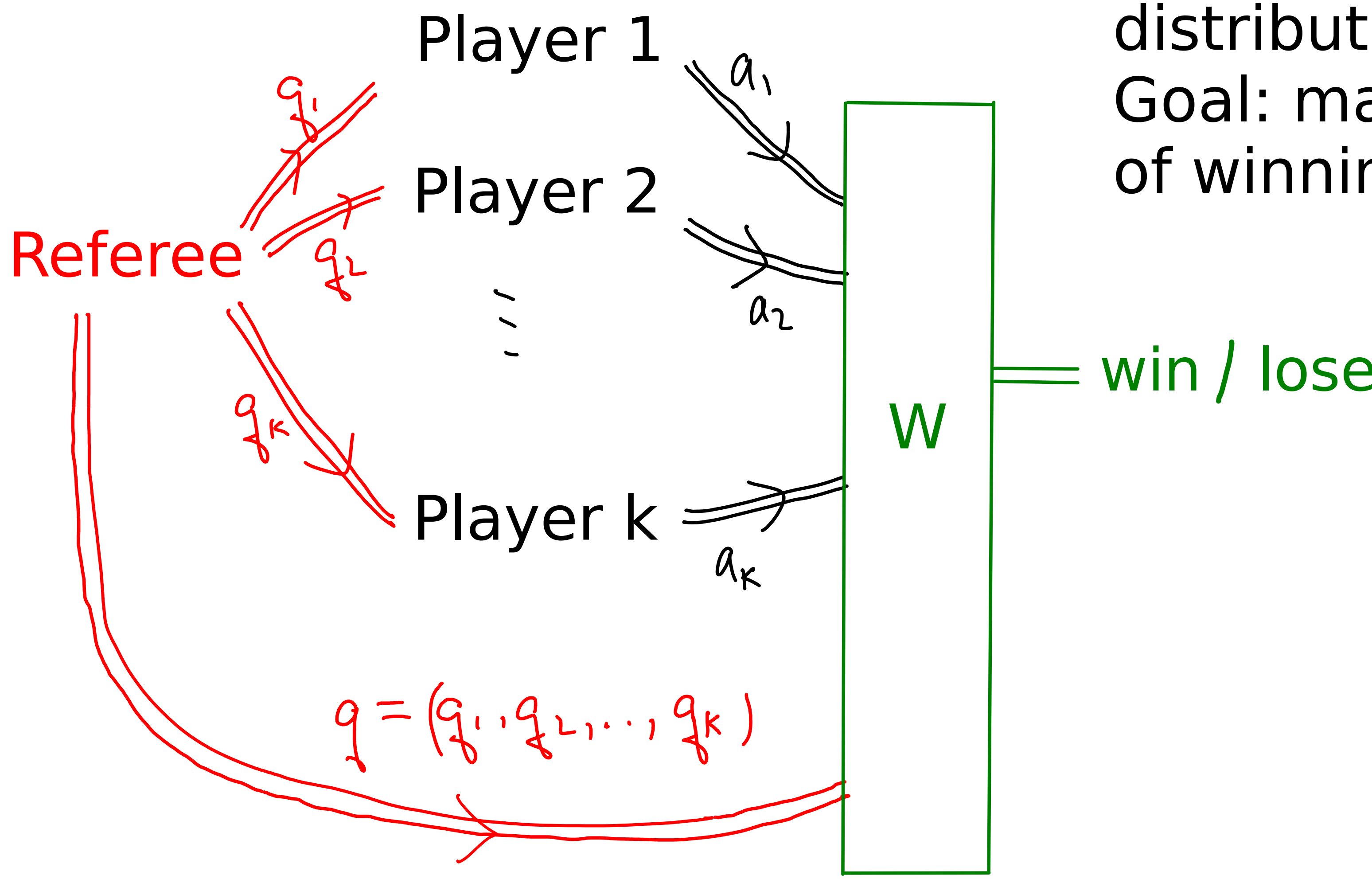
Zhengfeng Ji, Debbie Leung, Thomas Vidick

arXiv:1802.04926

ZJ: University of Technology Sydney
DL: University of Waterloo
TV: Caltech

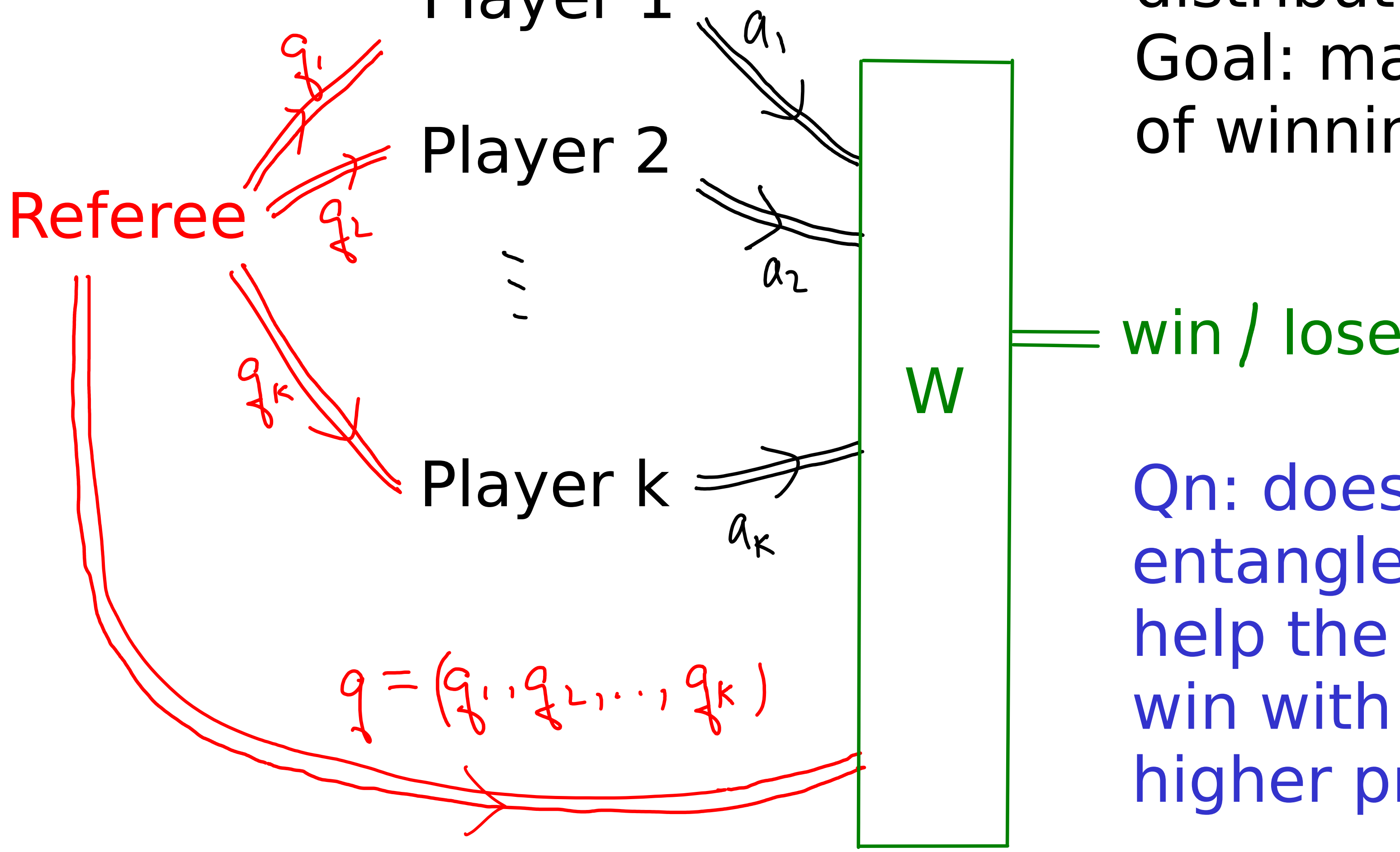
DL funding: NSERC, CIFAR

Nonlocal games



Players know W, distribution of q.
Goal: max prob of winning.

Nonlocal games

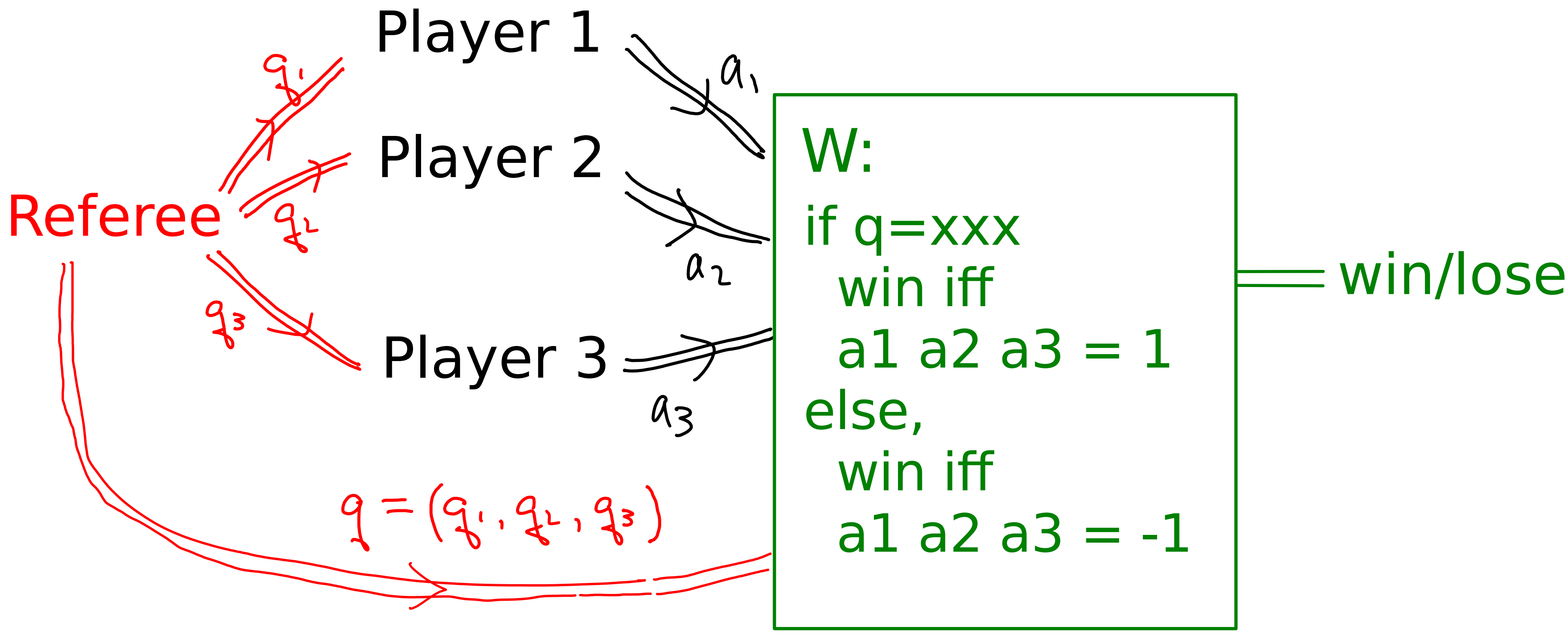


Players know W, distribution of q.
Goal: max prob of winning.

Qn: does sharing entanglement help the players win with strictly higher prob?

Example: GHZ game

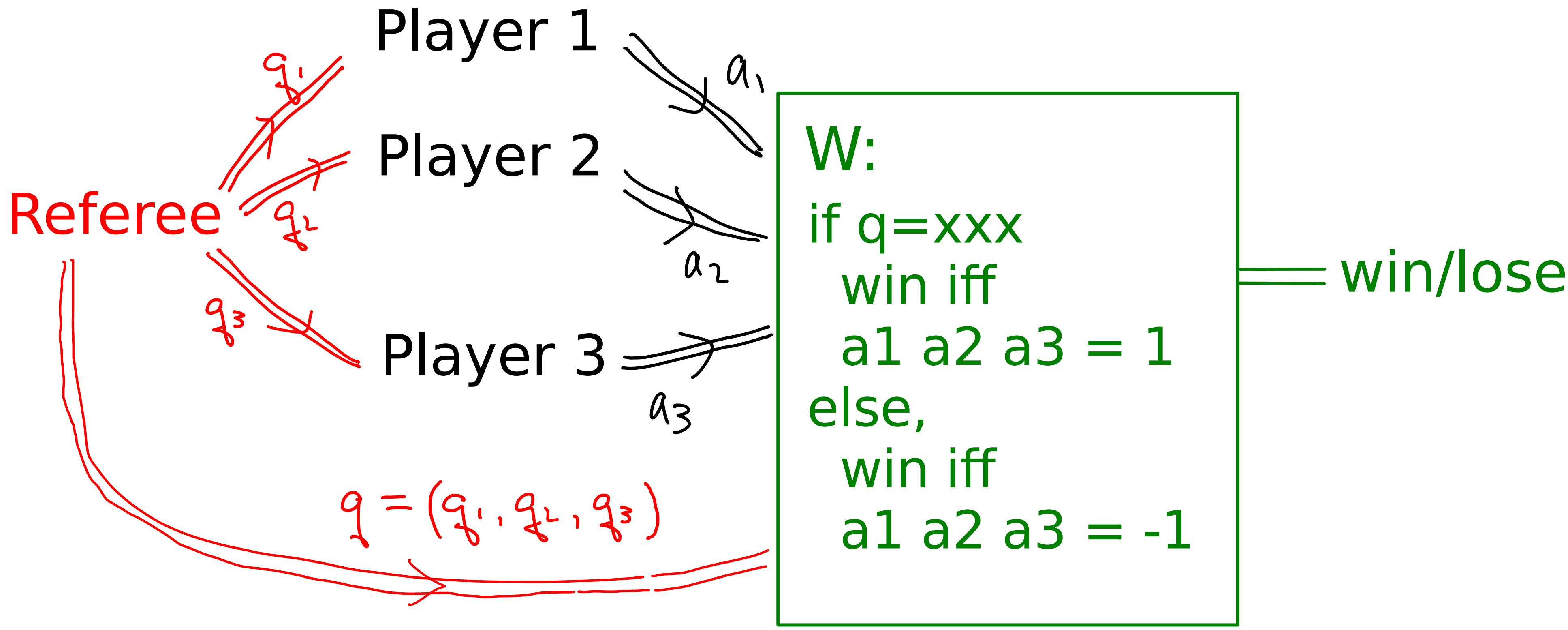
$k=3, \quad q \in_R \left\{ \begin{array}{l} (x,x,x), (y,y,x), \\ (y,x,y), (x,y,y) \end{array} \right\}$



The ith player receives a question $q_i \in \{x,y\}$, and provides an answer $a_i \in \{1,-1\}$.

Example: GHZ game

$k=3$, $q \in_R \{(x,x,x), (y,y,x), (y,x,y), (x,y,y)\}$



Without entanglement, winning prob <= 3/4.

With a GHZ state, each party measures Pauli-X (Y) given question x (y). The GHZ state is a +1 eigenstate of XXX, -1 eigenstate of XYY, YXY, YYX, so, winning prob = 1 !

Nonlocal games	Bell type experiments
Questions to a player	Measurement settings
Answers from a player	Measurement outcomes
Winning probability	Bell inequality
Classical strategy	Local hidden variables

shared randomness

Entangled strategy has strictly higher winning prob than classical strategy	Violation of Bell inequality

Why nonlocal games?

Computational complexity -
Expressive power of interactive proof systems and the effect due to entanglement

Physics -
QM vs Local Hidden Variable model

Crypto -
QKD via rigidity (uniqueness of optimal solution)

Fundamental question:
How much entanglement is required to win optimally?

Computational complexity:
Is MIP* = NEXP?

Operator algebra:
Is Connes embedding conjecture true? (This is about approx vN algebra with matrix algebra).

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Pal and Vertesi 09: I3322 game

"Simple": 2 players, 3 questions & 2 answers each, 12 queries, numerical evidence for conjecture, analytically elusive. (e.g., numerical optimal strategy uses ~5.8 ebits as the dim diverges, L, Wang, in prep).

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Sloftra 17:

Existential proof for the conjecture, 2 players, hundreds of questions & ans for each player.

Example not explicit and not answering "why/how" ...

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Sloftra 17:

Existential proof for the conjecture, 2 players, hundreds of questions & answers for each player.

Example not explicit and not answering "why/how" ...

Sloftra and Vidick 17: quantitative

ε close to optimal requires $\Omega(\varepsilon^{-k})$ - dim entangled state.

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Dykema, Paulsen, and Prakash 17:

Showed non-closure of correlations for 2 players, 5 questions and 2 answers each; use matrix analysis & irrational numbers. Almost but not explicit game.

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Today:

Explicit game, 3 parties, 12 questions, 8 or 4 ans each.
Elementary proof with physical reasons for non-closure.

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

Today:

Explicit game, 3 parties, 12 questions, 8 or 4 ans each. Elementary proof with physical reasons for non-closure.

Based on game in L, Toner, Watrous 08, with 2-parties, each with 3-dim quantum question and 2-dim quantum answer. We turn this to a nonlocal game.

LTW08 game explicit & based on embezzlement (van Dam and Hayden 02).

Problem since 2009:

If # questions and answers are finite for each player, is there an optimal strategy using a finite amount of entanglement ?

Conjecture: for some games, more entanglement wins with higher prob.

New development:
Coladangelo and Stark (1804.05116): explicit game with 2 players, 4 or 5 qns and 3 ans each (I4533).
Intriguing similarities to I3322 (e.g., dim diverges but entanglement converges).

Plan:

1. Embezzlement and its properties

2. Embezzlement game (LTW08)

3. Turning embezzlement game to a nonlocal game

4. Brief reasoning for soundness

1. Embezzlement and its properties:

Entanglement:

Conserved under local unitary operations.

In particular, $|00\rangle_{A'B'} \not\leftrightarrow |\phi\rangle_{A'B'}$ for any entangled $|\phi\rangle$,

and $|\psi\rangle_{AB}\, |00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$ for any $|\psi\rangle$ already shared.

1. Embezzlement and its properties:

Entanglement:

Conserved under local unitary operations.

In particular, $|00\rangle_{A'B'} \not\leftrightarrow |\phi\rangle_{A'B'}$ for any entangled $|\phi\rangle$,

and $|\psi\rangle_{AB}\, |00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$ for any $|\psi\rangle$ already shared.

Embezzlement of entanglement:

Theorem. $\forall\, \varepsilon > 0,\ \forall\, d,\ \forall\, |\phi\rangle_{A'B'} \in C^d \otimes C^d$

$\exists\, N,\ \exists\, |\psi\rangle_{AB} \in C^N \otimes C^N,$

$\exists\, U, V$ s.t. $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$!

any state $|\phi\rangle$
can be embezzled
(with local ops)
to any accuracy
given the right $|\psi\rangle$

van Dam & Hayden, quant-ph/0201041 (universal "catalyst", 2-party only, elementary 1-page proof.)

Alternative method (LTW08):

Catalyst depends on the initial & target states, but the local unitaries don't. Any # parties, other conserved quantities. Will see the proof (really short).

Aside: explains macroscopically controlled quantum gates, and relates to reference frames (0610030, 1804.03730).

Alternative (& obvious) embezzlement method

Goal: $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\, |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\, |\phi\rangle_{Ar+1Br+1} \cdots |\phi\rangle_{AnBn}$$

$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\, |\phi\rangle^{\otimes n-r}$$

Alternative (& obvious) embezzlement method

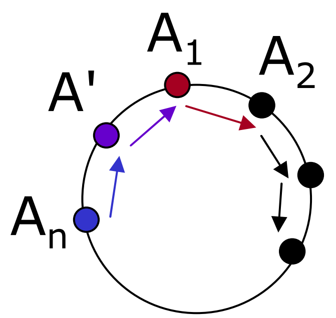
Goal: $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\, |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\, |\phi\rangle_{Ar+1Br+1} \ldots |\phi\rangle_{AnBn}$$

$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\, |\phi\rangle^{\otimes n-r}$$

2. $U_{AA'}$: cyclic permutation of systems



i.e. $U\, |i_1\rangle_{A1}\, |i_2\rangle_{A2} \ldots |i_n\rangle_{An}\, |i\rangle_{A'}$

$= |i\rangle_{A1}\, |i_1\rangle_{A2} \ldots |i_{n-1}\rangle_{An}\, |i_n\rangle_{A'}$

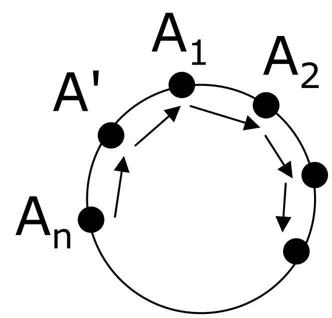
Alternative (& obvious) embezzlement method

Goal: $(U_{AA'} \otimes V_{BB'})\ |\psi\rangle_{AB}\ |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\ |\phi\rangle_{A'B'}$

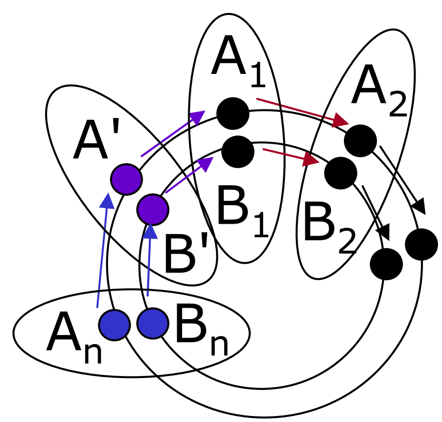
1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\ |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\ |\phi\rangle_{Ar+1Br+1} \cdots |\phi\rangle_{AnBn}$$
$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\ |\phi\rangle^{\otimes n-r}$$

2. $U_{AA'}$: cyclic permutation of systems



3. $V_{BB'}$ similar



i.e. $U\ |i_1\rangle_{A1}\ |i_2\rangle_{A2} \ldots |i_n\rangle_{An}\ |i\rangle_{A'}$
$= |i\rangle_{A1}\ |i_1\rangle_{A2} \ldots |i_{n-1}\rangle_{An}\ |i_n\rangle_{A'}$

Alternative (& obvious) embezzlement method

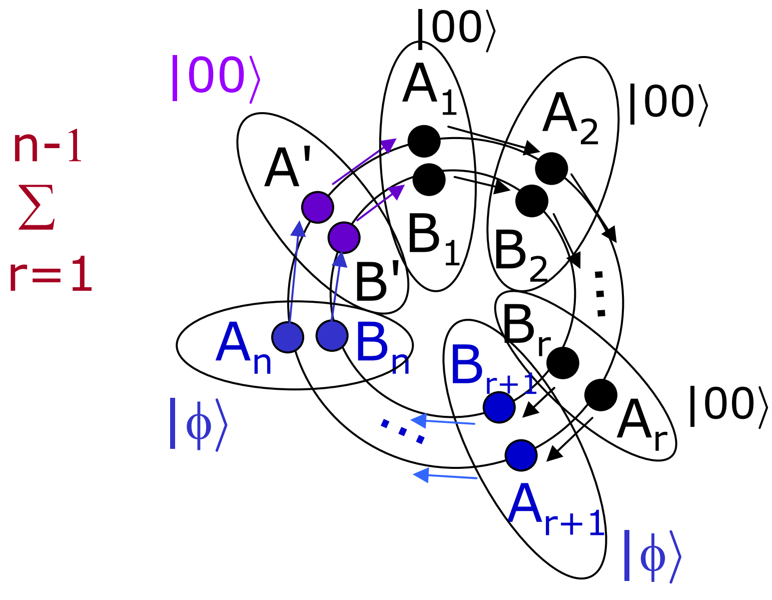
Goal: $(U_{AA'} \otimes V_{BB'})\ |\psi\rangle_{AB}\ |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\ |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\ |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\ |\phi\rangle_{Ar+1Br+1} \cdots |\phi\rangle_{AnBn}$$

$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\ |\phi\rangle^{\otimes n-r}$$

2. $(U_{AA'} \otimes V_{BB'})\ |\psi\rangle_{AB}\ |00\rangle_{A'B'}$



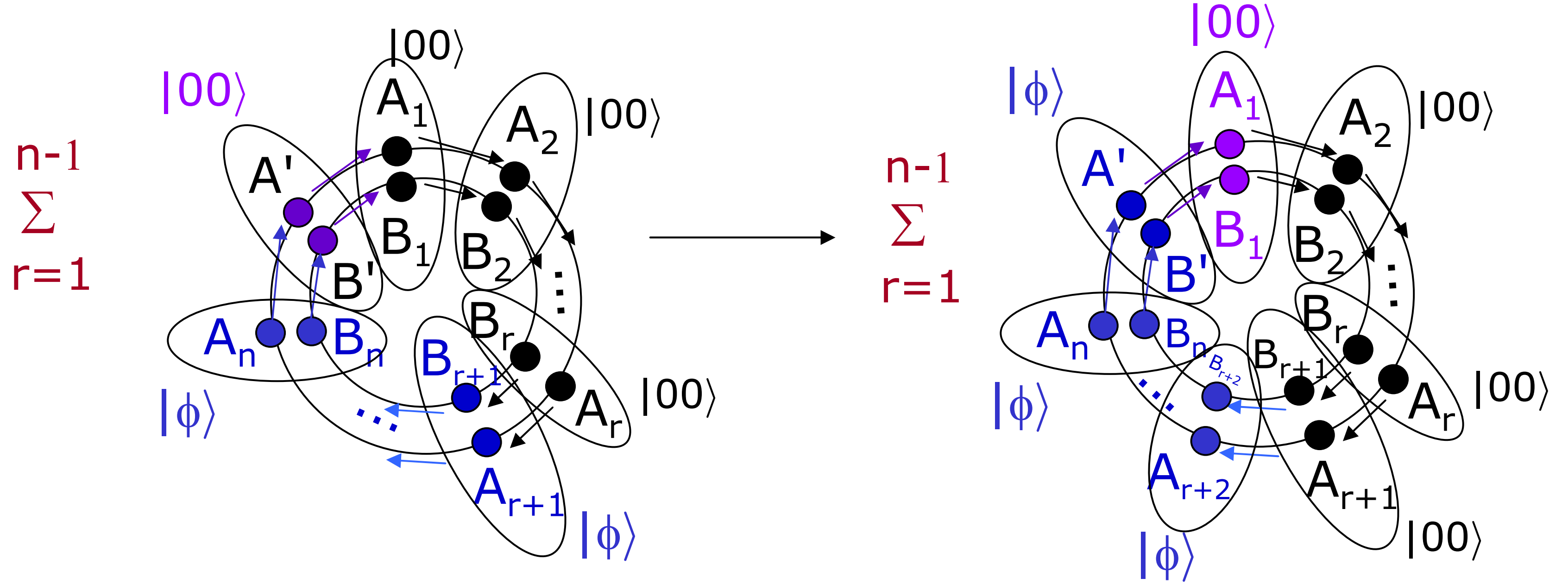
Alternative (& obvious) embezzlement method

Goal: $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\, |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\, |\phi\rangle_{Ar+1Br+1} \ldots |\phi\rangle_{AnBn}$$
$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\, |\phi\rangle^{\otimes n-r}$$

2. $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'}$



Alternative (& obvious) embezzlement method

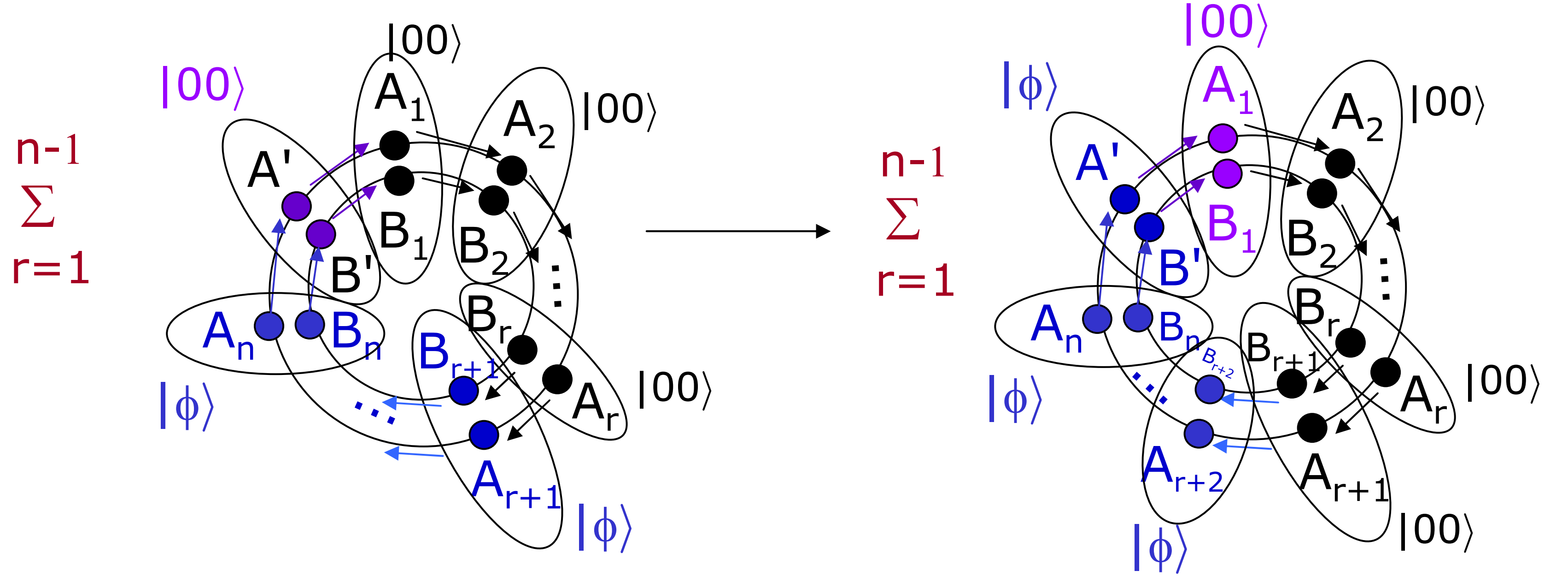
Goal: $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \dots A_n$, $B = B_1 \dots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\, |00\rangle_{A2B2} \dots |00\rangle_{ArBr}\, |\phi\rangle_{Ar+1Br+1} \cdots |\phi\rangle_{AnBn}$$

$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\, |\phi\rangle^{\otimes n-r}$$

2. $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} = (C \sum_{r=1}^{n-1} |00\rangle^{\otimes r+1}\, |\phi\rangle^{\otimes n-r-1})_{AB}\, |\phi\rangle_{A'B'}$



Alternative (& obvious) embezzlement method

Goal: $(U_{AA'} \otimes V_{BB'})\ |\psi\rangle_{AB}\ |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\ |\phi\rangle_{A'B'}$

1. Choose $A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, each $A_i \sim A'$, $B_i \sim B'$

$$|\psi\rangle_{AB} = C \sum_{r=1}^{n-1} |00\rangle_{A1B1}\ |00\rangle_{A2B2} \ldots |00\rangle_{ArBr}\ |\phi\rangle_{Ar+1Br+1} \cdots |\phi\rangle_{AnBn}$$

$$= C \sum_{r=1}^{n-1} |00\rangle^{\otimes r}\ |\phi\rangle^{\otimes n-r}$$

2. $$(U_{AA'} \otimes V_{BB'})\ |\psi\rangle_{AB}\ |00\rangle_{A'B'} = \underbrace{\left(C \sum_{r=1}^{n-1} |00\rangle^{\otimes r+1}\ |\phi\rangle^{\otimes n-r-1}\right)_{AB}}_{\substack{|\psi'\rangle_{AB} \text{ almost the same as } |\psi\rangle_{AB} \\ \text{with } r \to r+1}}\ |\phi\rangle_{A'B'}$$

$\langle\psi'|\psi\rangle_{AB} \geq 1\text{-}1/n \quad \therefore n = 1/\varepsilon$ suffices.

The impossibility and the possibility of embezzlement:

Qualitative no-go theorem: $|\psi\rangle_{AB}\ |00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\ |\phi\rangle_{A'B'}$

Possibility of approximate embezzlement :
poor "continuity" of the no-go theorem

But even a poor continuity bound still limits how well embezzlement can be approximated -- higher accuracy requires more dimensions in the catalyst!

Limits to embezzlement of entanglement:

Qualitative no-go theorem: $|\psi\rangle_{AB}\, |00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$

Quantitative

Theorem:

If $\varepsilon > 0$, $|\phi\rangle_{A'B'} \in C^d \otimes C^d$, $|\psi\rangle_{AB} \in C^N \otimes C^N$,

and $\exists$ U, V s.t. $\langle\psi|_{AB}\, \langle\phi|_{A'B'}\, (U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \geq 1 - \varepsilon$

then $\varepsilon \geq 8\, [\, E(|\phi\rangle) / (\log N + \log d)\,]^2$

Limits to embezzlement of entanglement:

Qualitative no-go theorem: $|\psi\rangle_{AB}\,|00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\,|\phi\rangle_{A'B'}$

Quantitative

Theorem:

If $\varepsilon > 0$, $|\phi\rangle_{A'B'} \in C^d \otimes C^d$, $|\psi\rangle_{AB} \in C^N \otimes C^N$,

and $\exists$ U, V s.t. $\langle\psi|_{AB}\,\langle\phi|_{A'B'}\,(U_{AA'} \otimes V_{BB'})\,|\psi\rangle_{AB}\,|00\rangle_{A'B'} \geq 1-\varepsilon$

then $\varepsilon \geq 8\,[\,E(|\phi\rangle) / (\log N + \log d)\,]^2$

Proof idea: compare $|\omega_1\rangle_{AA'BB'} = |\psi\rangle_{AB}\,|\phi\rangle_{A'B'}$

and $|\omega_2\rangle_{AA'BB'} = U_{AA'} \otimes V_{BB'}\,|\psi\rangle_{AB}\,|00\rangle_{A'B'}$

Fannes ineq

$$|\omega_1\rangle_{AA'BB'} \approx^{\varepsilon} |\omega_2\rangle_{AA'BB'} \Rightarrow E(|\omega_1\rangle) \approx^{f(\varepsilon)\log Nd} E(|\omega_2\rangle)$$

Limits to embezzlement of entanglement:

Qualitative no-go theorem: $|\psi\rangle_{AB}\,|00\rangle_{A'B'} \not\leftrightarrow |\psi\rangle_{AB}\,|\phi\rangle_{A'B'}$

Quantitative

Theorem:

If $\varepsilon > 0$, $|\phi\rangle_{A'B'} \in C^d \otimes C^d$, $|\psi\rangle_{AB} \in C^N \otimes C^N$,

and $\exists$ U, V s.t. $\langle\psi|_{AB}\,\langle\phi|_{A'B'}\,(U_{AA'} \otimes V_{BB'})\,|\psi\rangle_{AB}\,|00\rangle_{A'B'} \geq 1-\varepsilon$

then $\varepsilon \geq 8\,[\,E(|\phi\rangle)\,/\,(\log N + \log d)\,]^2$

Proof idea: compare $|\omega_1\rangle_{AA'BB'} = |\psi\rangle_{AB}\,|\phi\rangle_{A'B'}$

and $|\omega_2\rangle_{AA'BB'} = U_{AA'} \otimes V_{BB'}\,|\psi\rangle_{AB}\,|00\rangle_{A'B'}$

Fannes ineq

$$|\omega_1\rangle_{AA'BB'} \overset{\varepsilon}{\approx} |\omega_2\rangle_{AA'BB'} \Rightarrow E(|\omega_1\rangle) \overset{f(\varepsilon)\log Nd}{\approx} E(|\omega_2\rangle)$$

$$\varepsilon \geq f^{-1}\left(\frac{E(|\phi\rangle)}{\log Nd}\right) \Leftarrow E(|\omega_1\rangle) - E(|\omega_2\rangle) \geq E(|\phi\rangle)$$

Plan:

1. Embezzlement and its properties

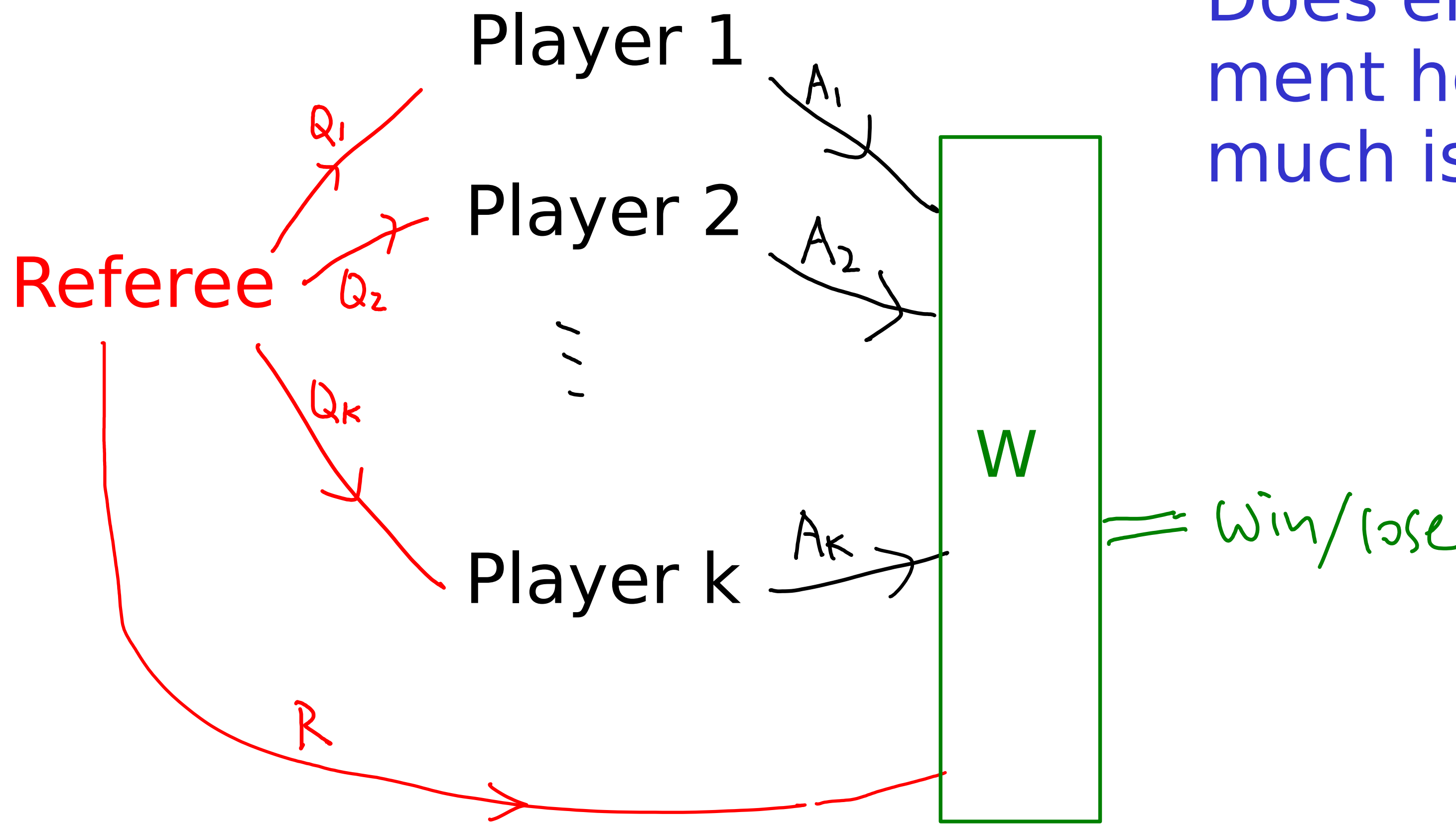
2. Embezzlement game (LTW08)

3. Turning embezzlement game to a nonlocal game

4. Brief reasoning for soundness

2. "Nonlocal game" with quantum questions & answers

Does entanglement help? How much is needed?



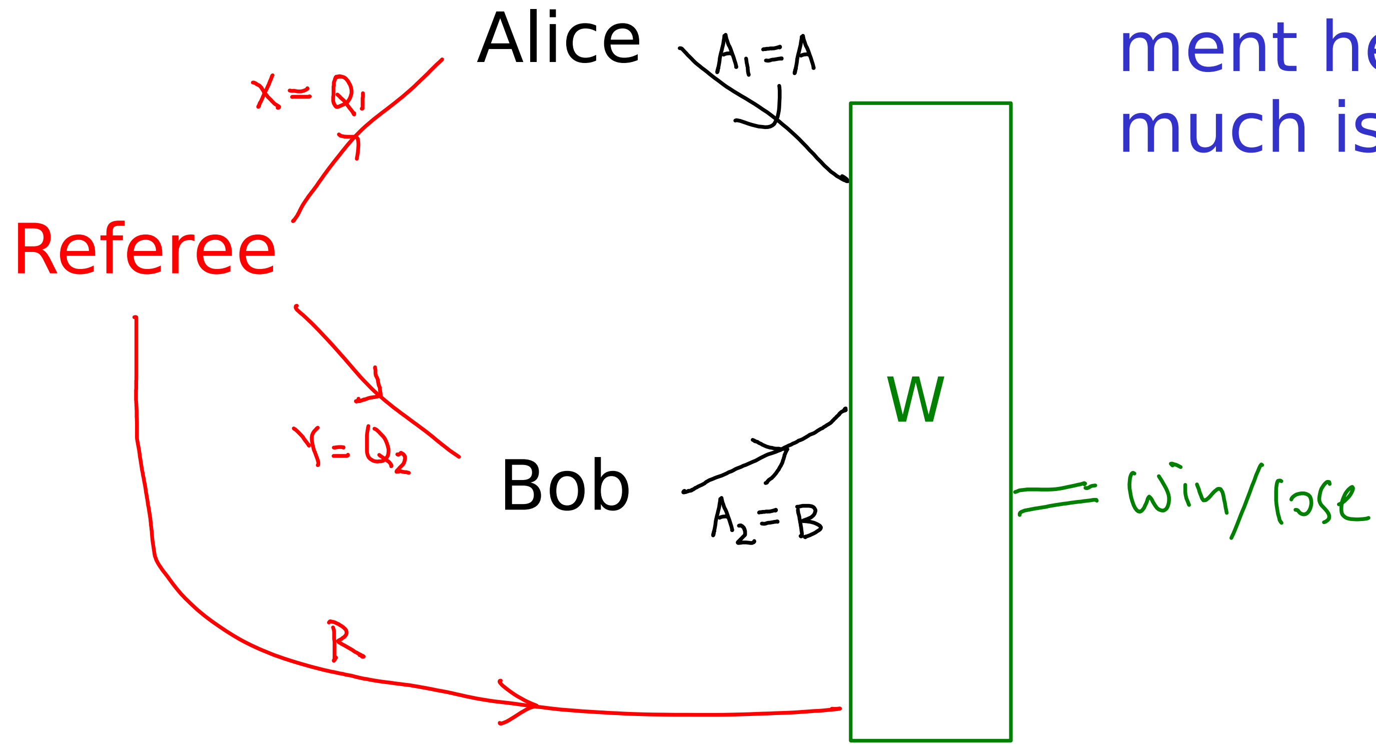
Initial pure state on R Q1 Q2 ... Qk

2-outcome POVM meas

known to the players

2. For 2 parties:

Does entanglement help? How much is needed?



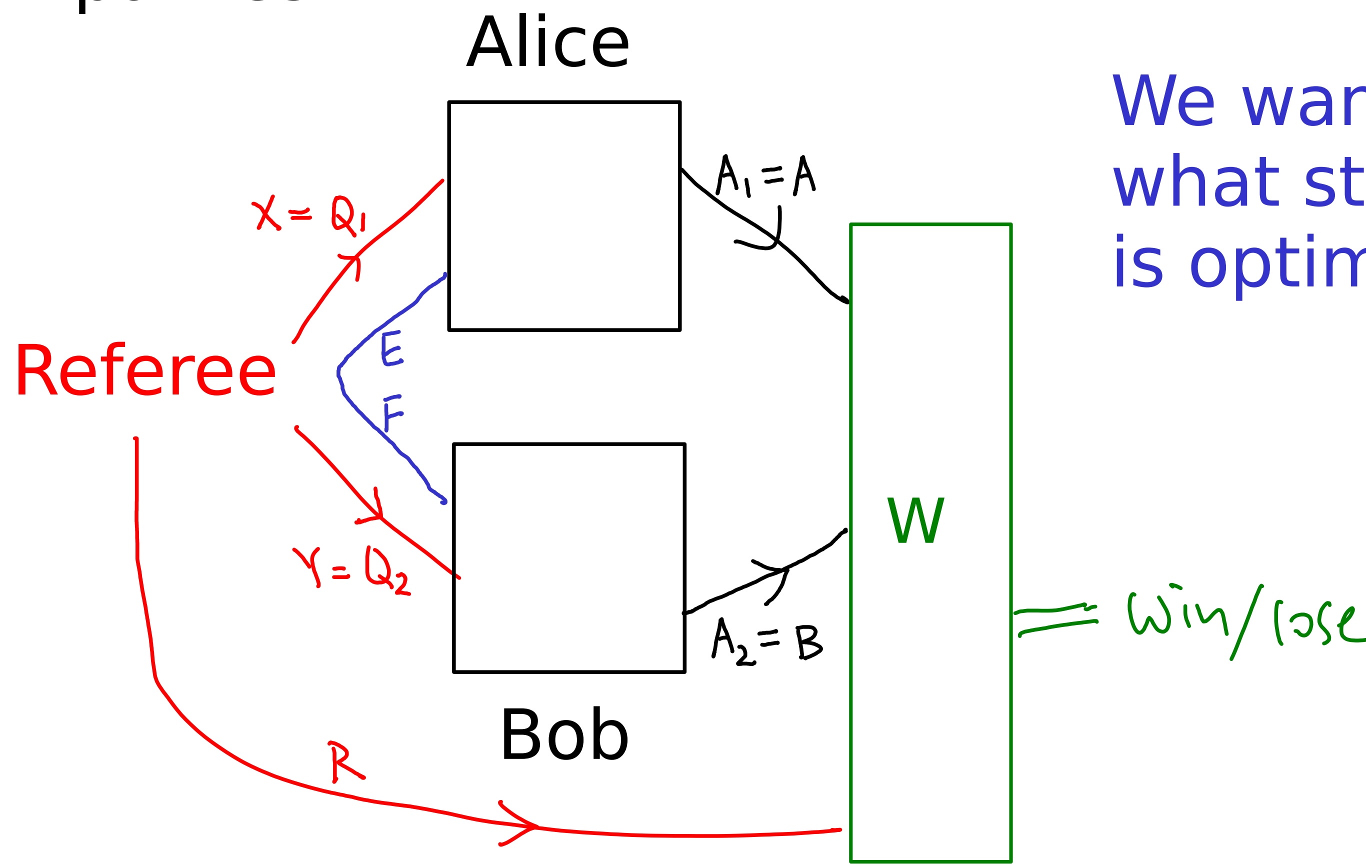
Initial pure state on R Q1 Q2 ... Qk

2-outcome POVM meas

known to the players

2. For 2 parties:

We want to know what states in EF is optimal.

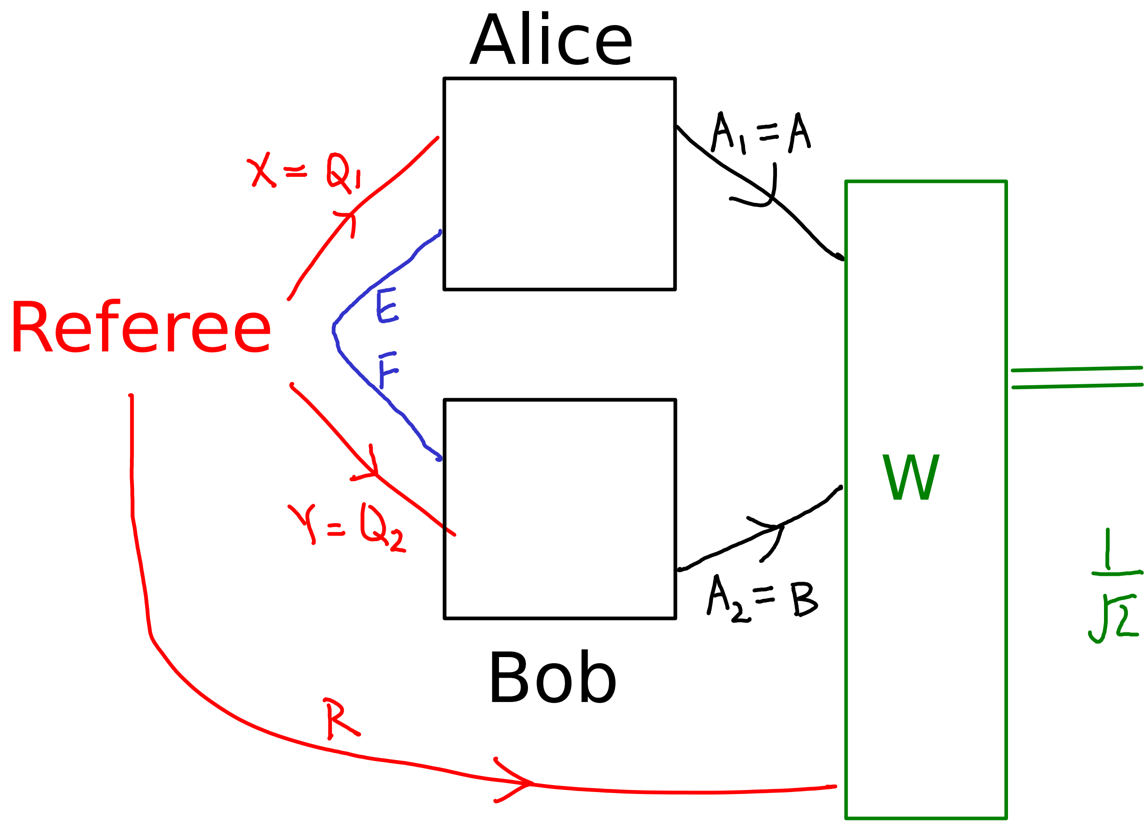


Initial pure state on RXY

2-outcome POVM meas

known to Alice and Bob

2. Embezzlement game that cannot be won with finite amount of entanglement (LTW08)



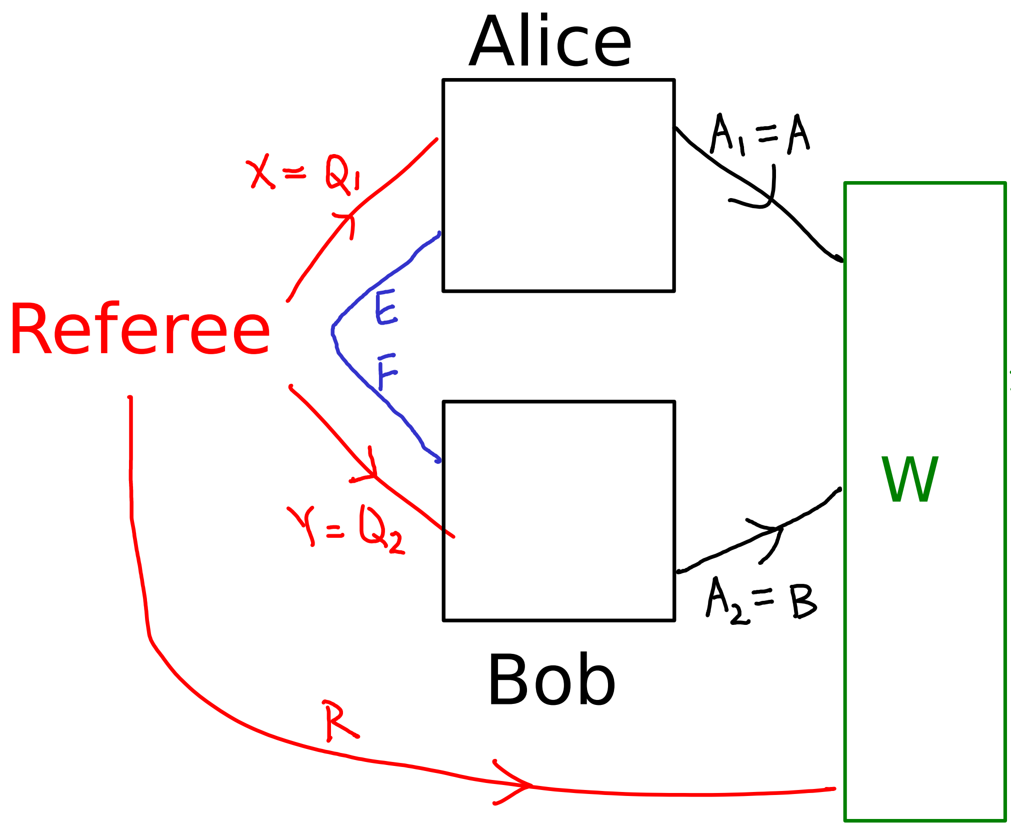
win iff projected onto the GHZ state

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle|11\rangle\right]_{RAB}$$

Initial state on RXY

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle\left(|22\rangle+|11\rangle\right)\frac{1}{\sqrt{2}}\right]_{RXY}$$

2. Embezzlement game that cannot be won with finite amount of entanglement (LTW08)



win iff projected onto the GHZ state

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle|11\rangle\right]_{RAB}$$

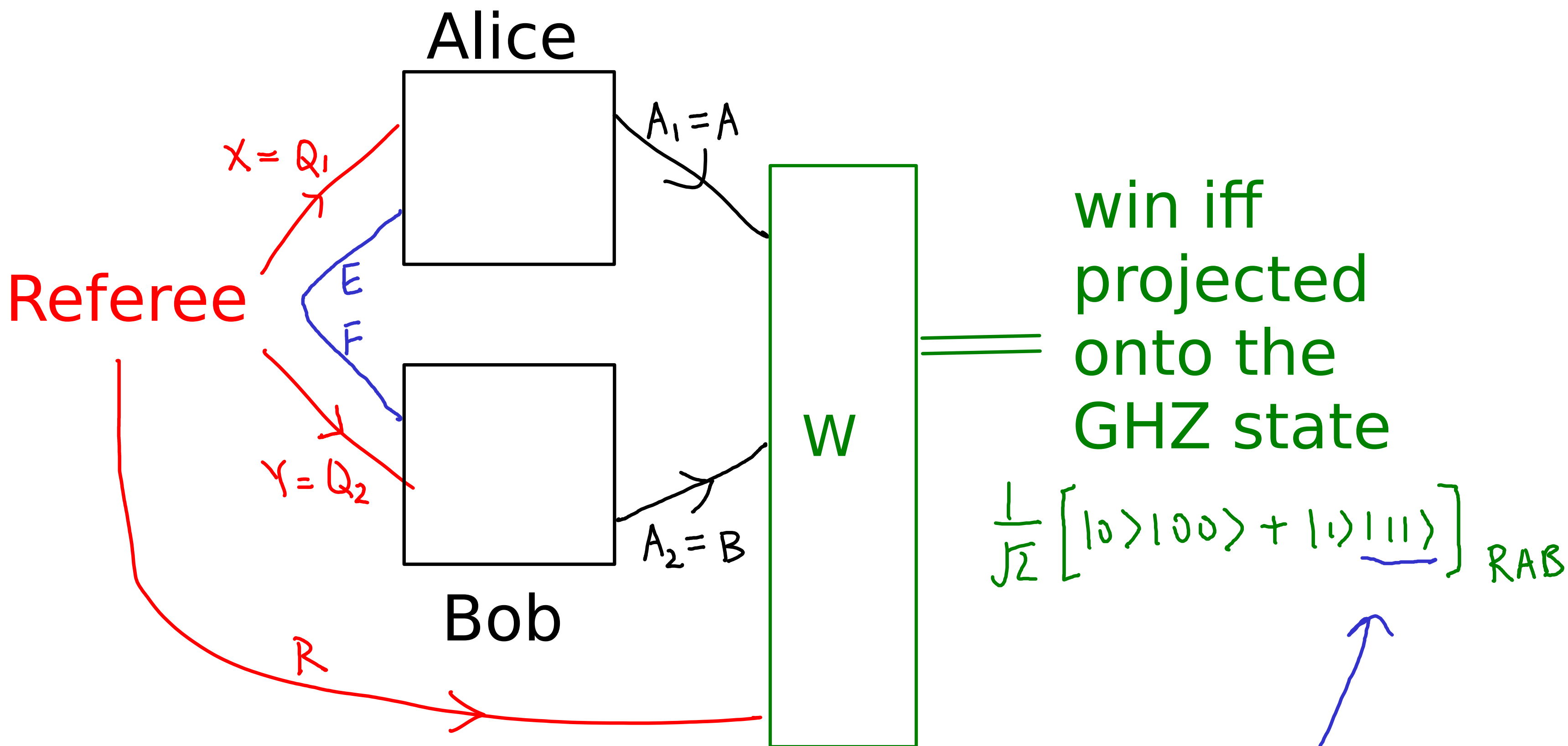
Initial state on RXY

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle\left(|22\rangle+|11\rangle\right)\frac{1}{\sqrt{2}}\right]_{RXY}$$

Strategy: conditioned on X (Y) in span$\{|1\rangle, |2\rangle\}$, Alice (Bob) reverse-embezzle $|11\rangle$ from $|\Phi\rangle$.

win prob -> 1

2. Embezzlement game that cannot be won with finite amount of entanglement (LTW08)



Initial state on RXY

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle\left(|22\rangle + |11\rangle\right)\frac{1}{\sqrt{2}}\right]_{RXY}$$

Strategy: conditioned on X (Y) in span$\{|1\rangle, |2\rangle\}$, Alice (Bob) reverse-embezzle $|11\rangle$ from $|\Phi\rangle$.

win prob -> 1

No other way to win:
win prob < 1- $\log^{-2}$ dim(E)

Plan:

1. Embezzlement and its properties

2. Embezzlement game (LTW08)

3. Turning embezzlement game to a nonlocal game

4. Brief reasoning for soundness

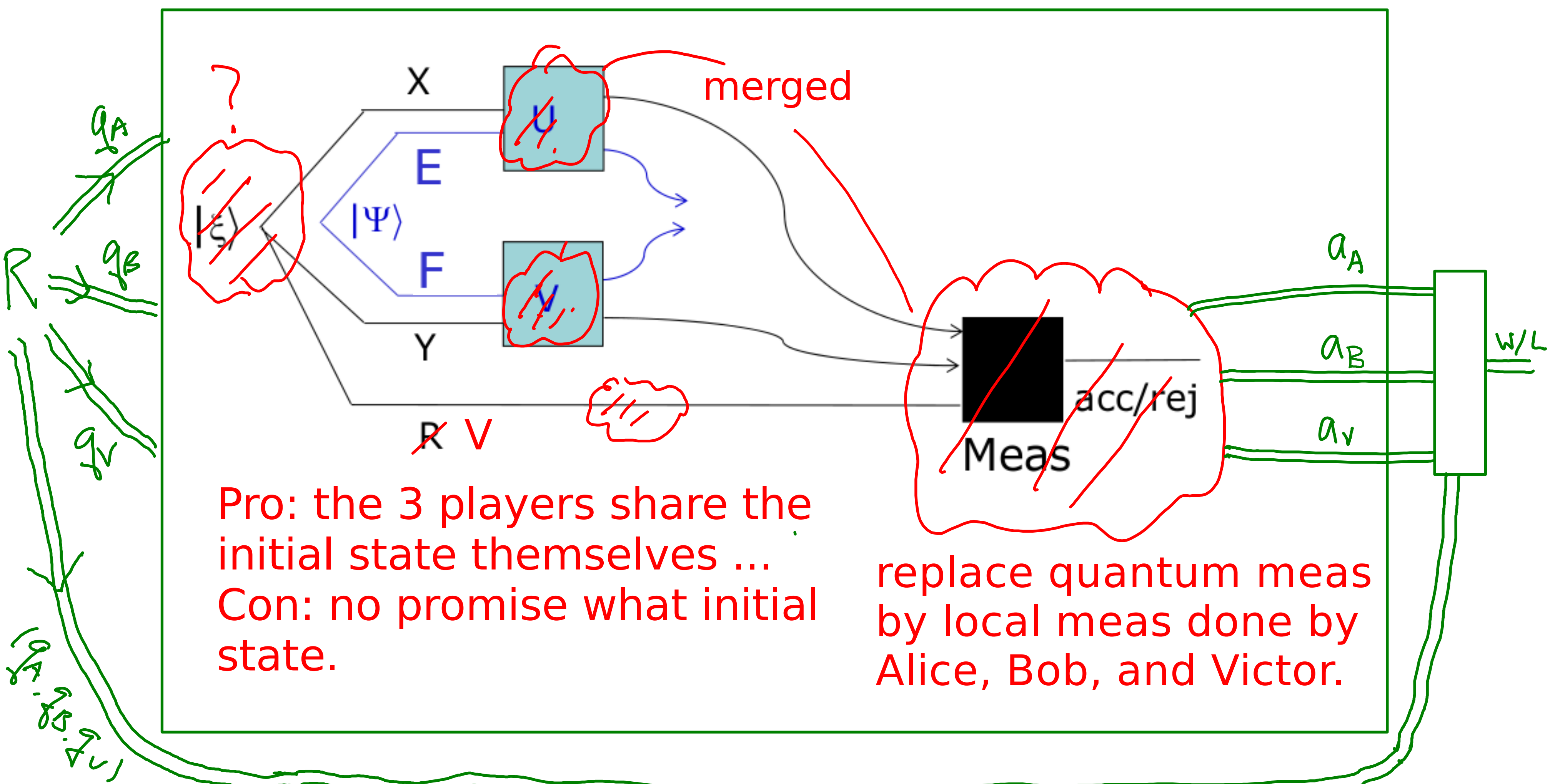
3. Modification of the embezzlement game to a nonlocal game

How to turn the questions and answers classical yet the parties still have to embezzle (so more entanglement is always better)?

Regev, Vidick 1207.4939:
Turned R, A, B classical, but X, Y remain quantum.

New idea:

Turn the 2-player embezzlement game into a 3-player nonlocal game, such that the original referee becomes a 3rd player (Victor). Add a new referee for the new nonlocal game (3EMB).



How to pick queries and winning conditions so that:
if Alice, Bob, and Victor want to win with near certainty, they must share the initial state for the embezzlement game and Alice-n-Bob must reverse-embezzle as before?

How to pick queries and winning conditions so that:
if Alice, Bob, and Victor want to win with near certainty, they must share the initial state for the embezzlement game and Alice-n-Bob must reverse-embezzle as before?

New ingredient:

A test P3 for 3 players: in this test, each player can be asked one of 6 possible questions. To win with high prob, they have to share 2 GHZ states and measure in X and Z (up to local isometries).

Obtained by merging the GHZ game with the Magic Square game ...

want:

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle\left(|22\rangle+|11\rangle\right)\frac{1}{\sqrt{2}}\right]_{VAB}$$

$$\downarrow$$

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle|11\rangle\right]_{VAB}$$

or equivalently:

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle|00\rangle + |1\rangle|11\rangle\left(|00\rangle+|11\rangle\right)\frac{1}{\sqrt{2}}\right]_{V_1A_1B_1\,A_2B_2}$$

$\downarrow$ Want

$$\frac{1}{\sqrt{2}}\left[|0\rangle|00\rangle + |1\rangle|11\rangle\right]_{V_1A_1B_1}$$

Try the following instead:

Enforce initial state (2 GHZs):

$$\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_1A_1B_1}\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_2A_2B_2}$$

Enforce an additional controlled-Hadamard from V1 to V2

$$\frac{1}{2}\Big[|0\rangle|00\rangle_{V_1A_1B_1}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_2A_2B_2} + |1\rangle|11\rangle_{V_1A_1B_1}\Big[\frac{|0\rangle+|1\rangle}{\sqrt{2}}|00\rangle + \frac{|0\rangle-|1\rangle}{\sqrt{2}}|11\rangle\Big]_{V_2A_2B_2}\Big]$$

$\|$ conditioned on $|0\rangle_{V_2}$

$$\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle|00\rangle + |1\rangle|11\rangle\big(|00\rangle+|11\rangle\big)\frac{1}{\sqrt{2}}\Big]_{V_1A_1B_1A_2B_2}$$

$\downarrow$ Want

$$\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_1A_1B_1}$$

$//$

Enforce the final state:
(2 GHZs)

$$\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_1A_1B_1}\frac{1}{\sqrt{2}}\Big[|0\rangle|00\rangle + |1\rangle|11\rangle\Big]_{V_3A_3B_3}$$

The nonlocal game 3EMB:

Each player receives a question from P3, Victor receives also a bit v, Alice and Bob both receive the same bit w.

	V v	A/B w	Queries & win conditions	Rigidity achieved
(a)	0	0	P3 on V1A1B1 and V2A2B2	GHZ on V1A1B1, V2A2B2 X,Z measurements
(b)	1	0	Victor must apply c-H on V1V2 & meas V2 honestly	wp 1/2, postmeas strate on V1A1B1A2B2 = initial state for embezzlement game
(c)	1	1	P3 on V1A1B1 and V3A3B3	Alice, Bob need to reverse-embezzle to prepare GHZ on V1A1B1

Victor cannot tell (b) from (c)

Alice, Bob cannot tell (a) from (b)

Qns similar for (a)-(c)

The referee interacts with three players, labeled P_V, P_A and P_B. Each player receives a question taken from the set $\{0,1\} \times \mathcal{Q}$, where $\mathcal{Q}$ is specified in (3). We use the symbol π_V, π_A, π_B to denote the first component (lying in $\{0,1\}$) of the question to P_V, P_A and P_B respectively. It will always be the case that $\pi_A = \pi_B = \pi$. In the game, P_V should reply with 3 bits $(u,v) \in \{0,1\} \times \{\pm 1\}^2$, while P_A, P_B each reply with 2 bits $a, b \in \{\pm 1\}^2$ respectively. Let $v = (v_1, v_2), a = (a_1, a_2), b = (b_1, b_2)$.

The referee performs either of the following tests chosen at random with equal probability:

(a) The referee sets $\pi_V = \pi = 0$. He executes the test P3 with the three players, inserting the question from P3 as the second component of their question, and checking validity of the triple (v,a,b) extracted from the players' answers as would the verifier in P3.

(b) The referee sets $\pi_V = 1$ and $\pi = 0$. The second component of P_V's question is chosen uniformly at random from $\mathcal{Q}$. The referee performs either of the following with equal probability:

  (i) Send both P_A and P_B the question r_2. Let a_1 and a_2 be the answers associated with entries iz and zi respectively. Reject if $a_1 = 1$ and (($u = 0$ and $a_2 = -1$) or ($u = 1$ and $a_2 = 1$)). Accept in all other cases.

  (ii) Send both P_A and P_B the question c_1. Let a_1 and a_2 be the answers associated with entries xi and iz respectively. Reject if $a_2 = -1$ and (($u = 0$ and $a_1 b_1 = -1$) or ($u = 1$ and $a_1 b_1 = 1$)). Accept in all other cases.

~~(c)~~ The referee sets $\pi_V = 1$ and $\pi = 0$. He sets the second component of P_V's question to r_2. He sends both P_A and P_B the same question, r_2. The referee rejects if $a_1 \neq v_2$ or $b_1 \neq v_2$.

(c)

~~(d)~~ The referee sets $\pi_V = \pi = 1$, and executes the test P3 as in part (a). If $u = 0$ the referee accepts if and only if the players' answers (v,a,b) pass the test P3. If $u = 1$ the referee always accepts.

Summary:

Our 3-player game [with 12 qns to each player, 3-bit ans from Victor, 2-bit ans from each of Alice and Bob] satisfies the following:

1. win wp > 1-e using ent state with 3 qubits held by Victor and O(1/e) qubits held by each of Alice, Bob.

2. win wp > 1-e requires ent state with at least $\Omega(e^{-1/32})$ qubits held by some parties.

Open problems:

1. Can we prove that I3322 is an example for the conjecture, and if so, is the reason related to that in the I4533 by Coladangelo and Stark?

2. For the quantum game, if we fix the dims for the questions and answers, find an upper bound for the dim of the entangled state as a function of e, where the winning prob is e from optimal?

3. For the complexity class MIP*, is there a bound on the entanglement required? What is MIP*?

4. The multi-party embezzlement catalyst can be made universal in a very inefficient way. Is there a more efficient catalyst?