

Title: Embezzlement of entanglement

Speakers: Debbie Leung

Series: Colloquium

Date: May 28, 2019 - 11:00 AM

URL: <http://pirsa.org/19050012>

Abstract: Embezzlement of entanglement is the (impossible) task of producing an entangled state from a product state via a local change of basis, when a suitable catalytic entangled state is available. The possibility to approximate this task was first observed by van Dam and Hayden in 2002. Since then, the phenomenon is found to play crucial roles in many aspects of quantum information theory. In this colloquium, we will explain various methods to embezzlement entanglement and explore applications (such as an extension to approximately violate other conservation laws, a Bell inequality that cannot be violated maximally with finite amount of entanglement, consequences for resource theories, and the quantum reverse Shannon theorem).

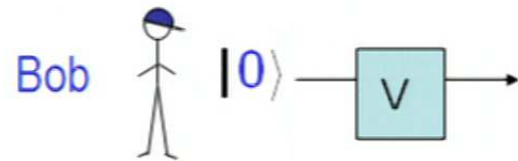
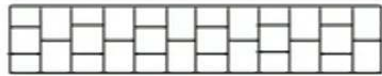
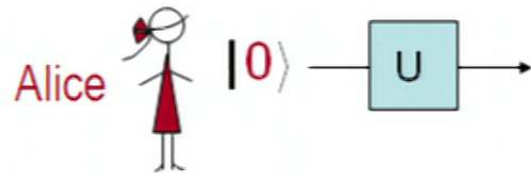
Embezzlement of entanglement

PI Colloquium, May 28, 2019

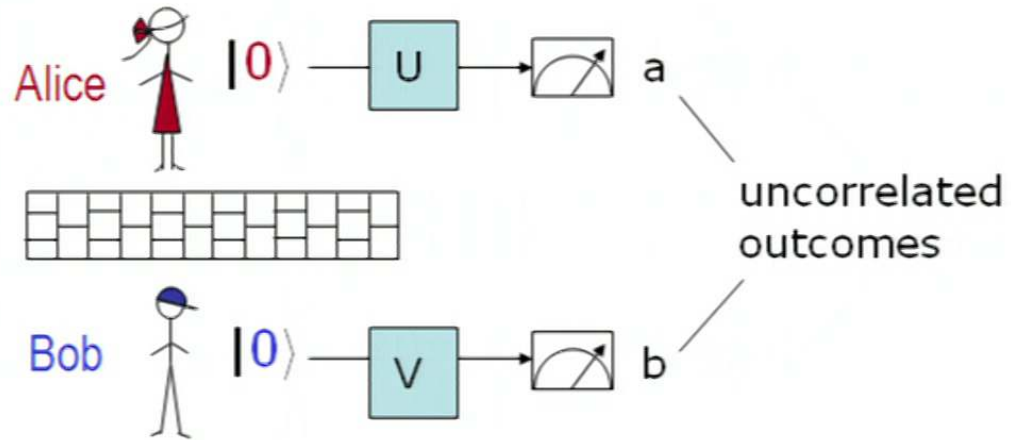
Debbie Leung

IQC and C&O, University of Waterloo

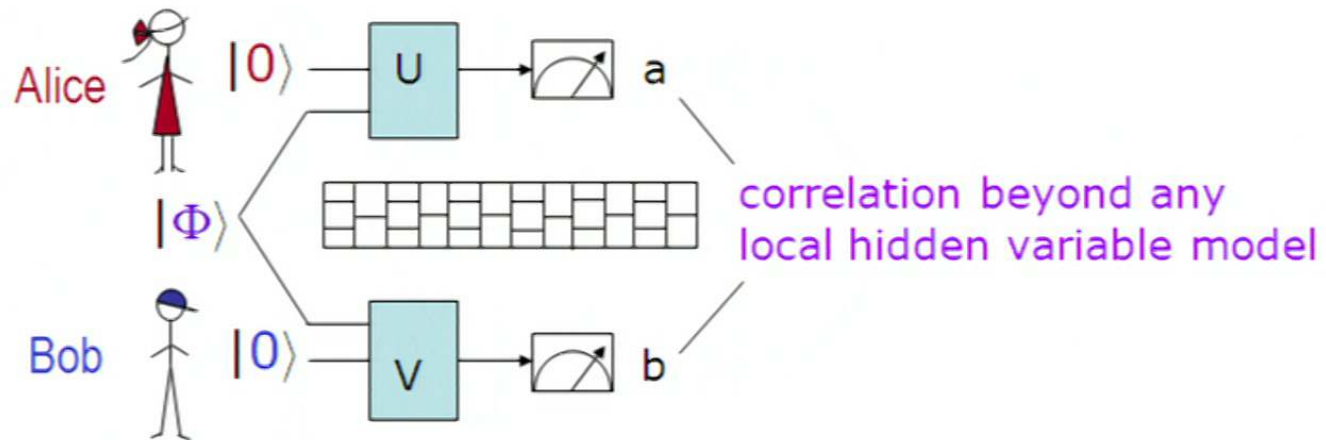
Local operations:



Local operations:

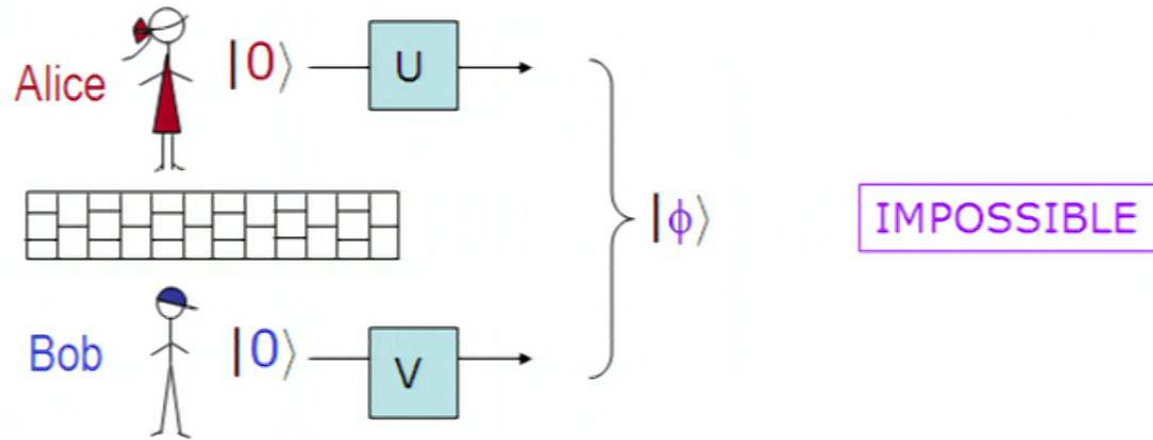


Entanglement:

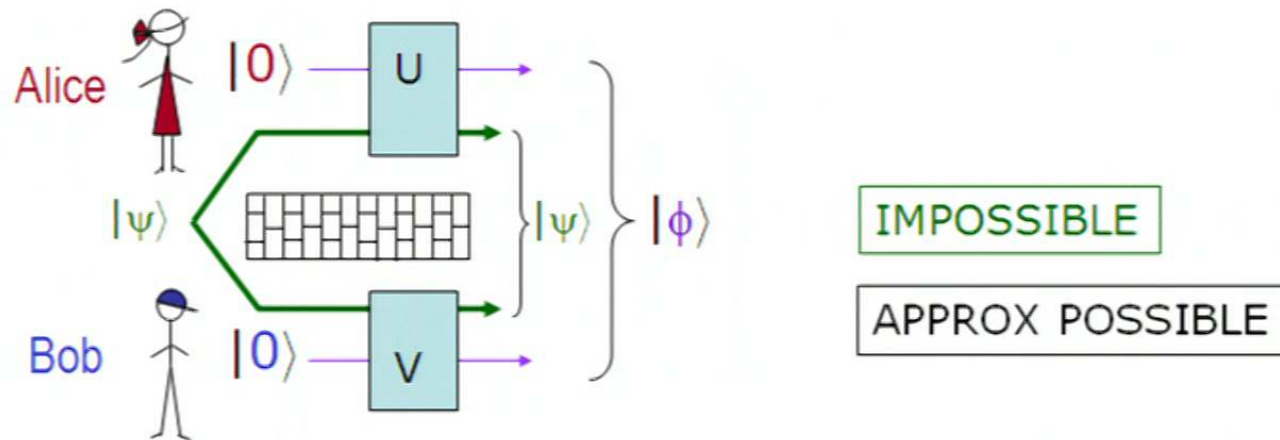


e.g., $|\Phi\rangle \propto |00\rangle + |11\rangle$

No free entanglement:



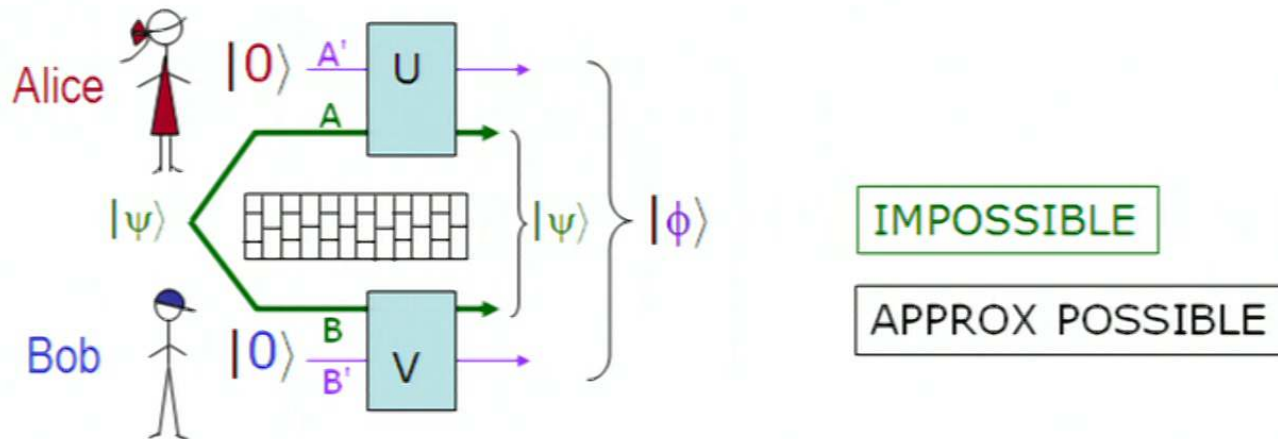
No free entanglement even with a catalyst:



Embezzlement of entanglement:

Any state $|\phi\rangle$ can be embezzled to any accuracy w/ some $|\psi\rangle$.

No free entanglement even with a catalyst:



Embezzlement of entanglement:

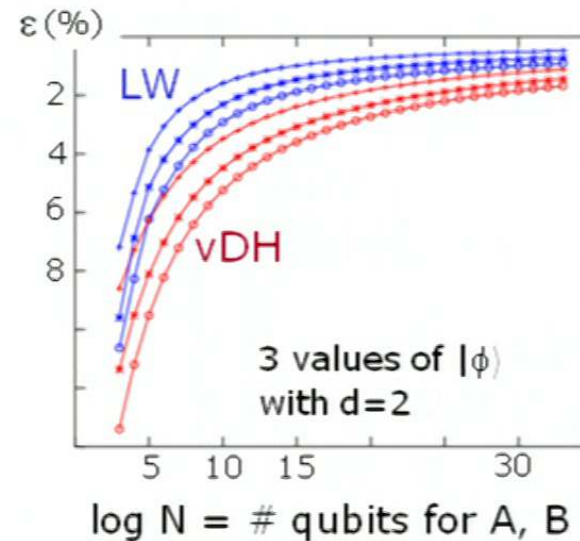
Any state $|\phi\rangle$ can be embezzled to any accuracy w/ some $|\psi\rangle$.

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

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

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

van Dam & Hayden 2002
 - conceived such possibility !
 - scheme with universal $|\psi\rangle$
 \forall 2-party $|\phi\rangle$ of fixed dim.



Embezzlement of entanglement:

Any state $|\phi\rangle$ can be embezzled to any accuracy w/ some $|\psi\rangle$.

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

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

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

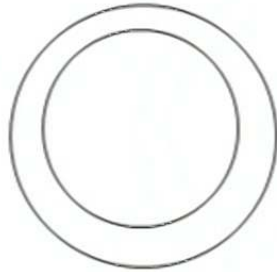
Alternative (& obvious) embezzlement scheme

Want: $(U_{AA'} \otimes V_{BB'}) |\psi\rangle_{AB} |00\rangle_{A'B'} \approx^\epsilon |\psi\rangle_{AB} |\phi\rangle_{A'B'}$ L, Toner, Watrous 08

Alternative (& obvious) embezzlement scheme

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

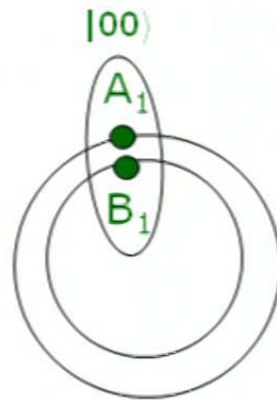
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

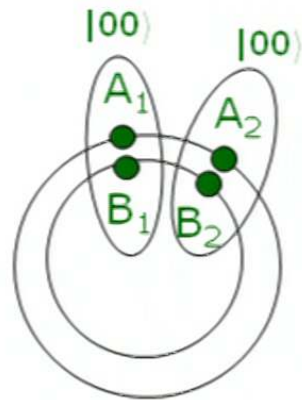
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

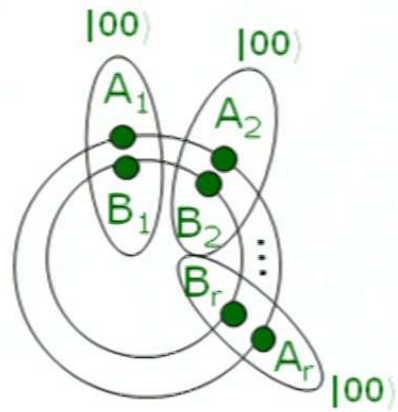
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

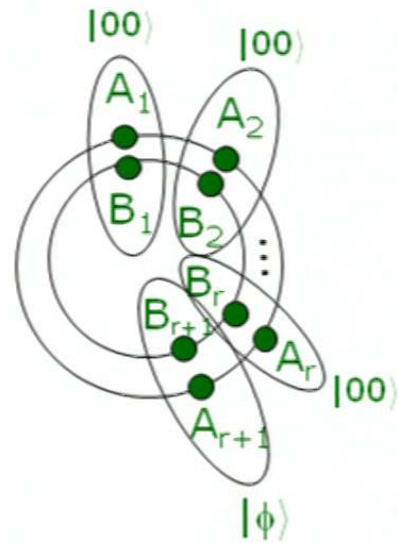
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

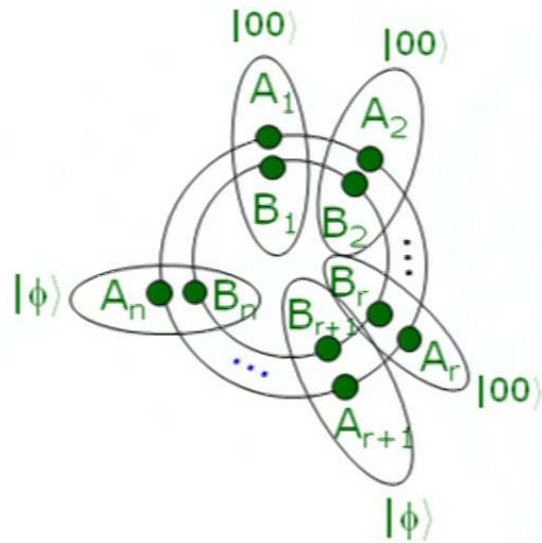
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

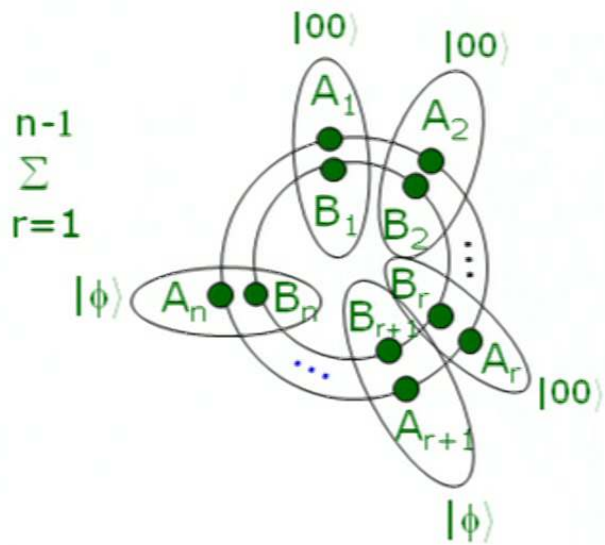
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

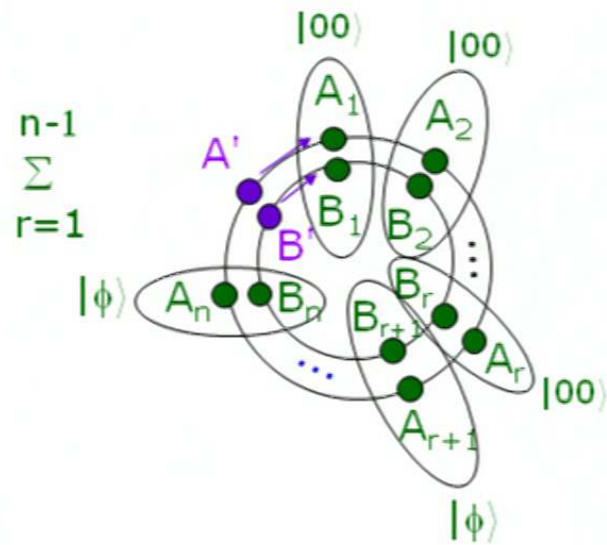
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

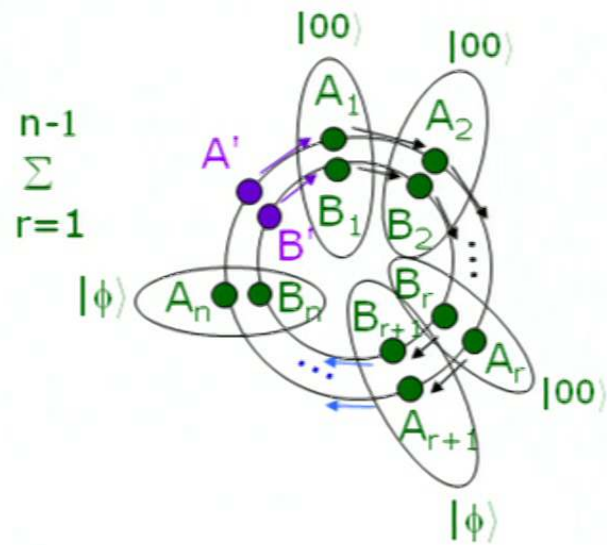
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

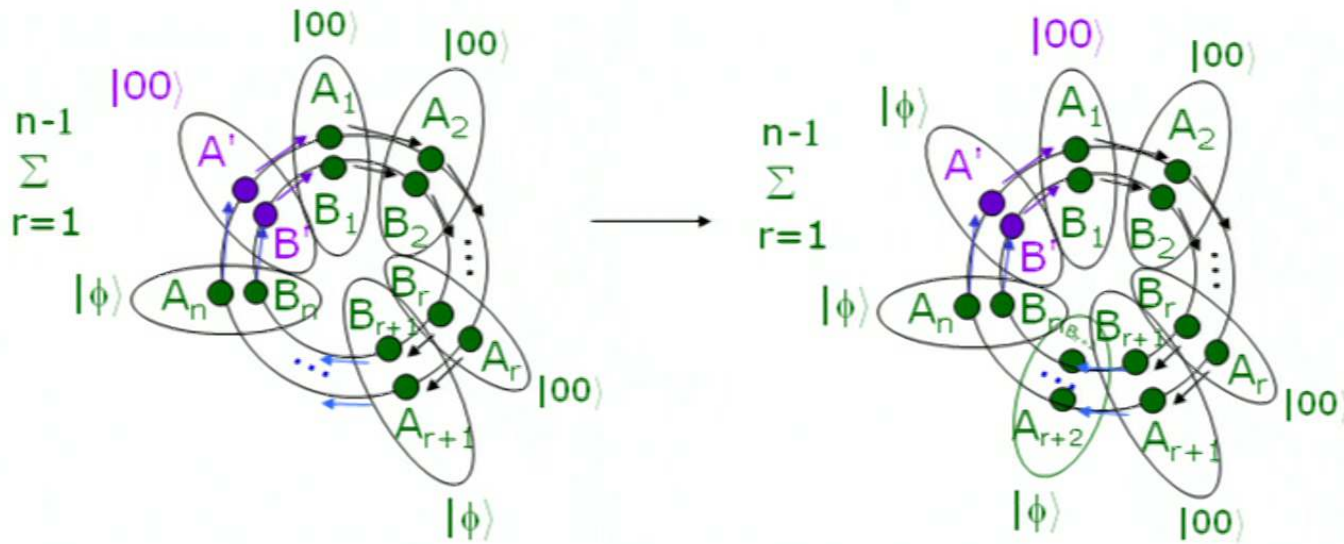
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

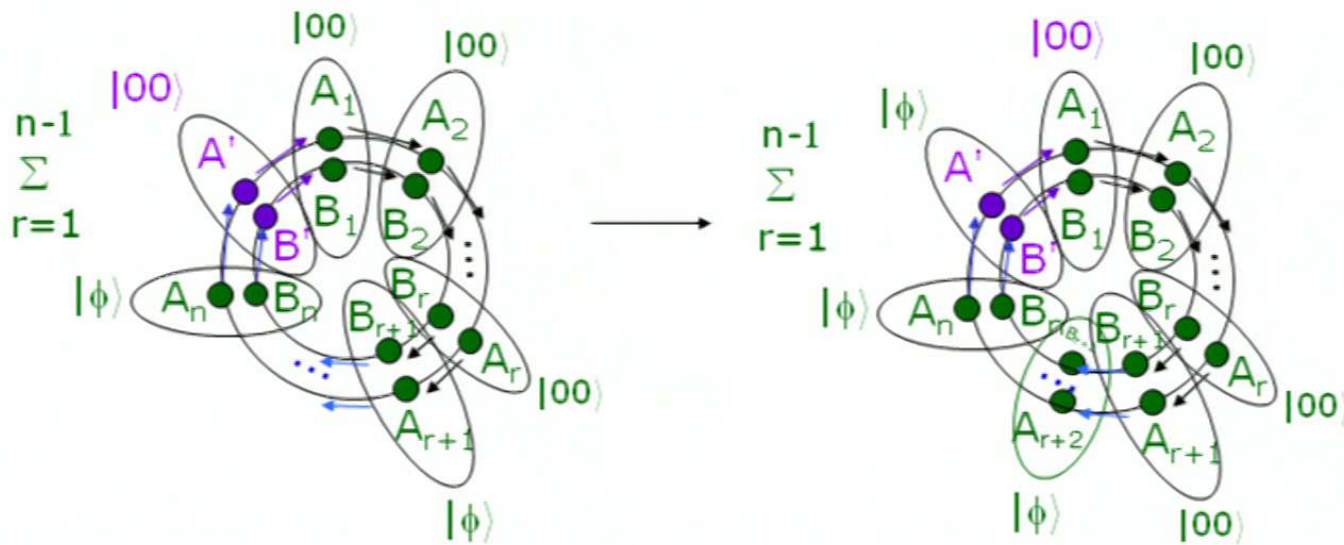
Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



Alternative (& obvious) embezzlement scheme

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

Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



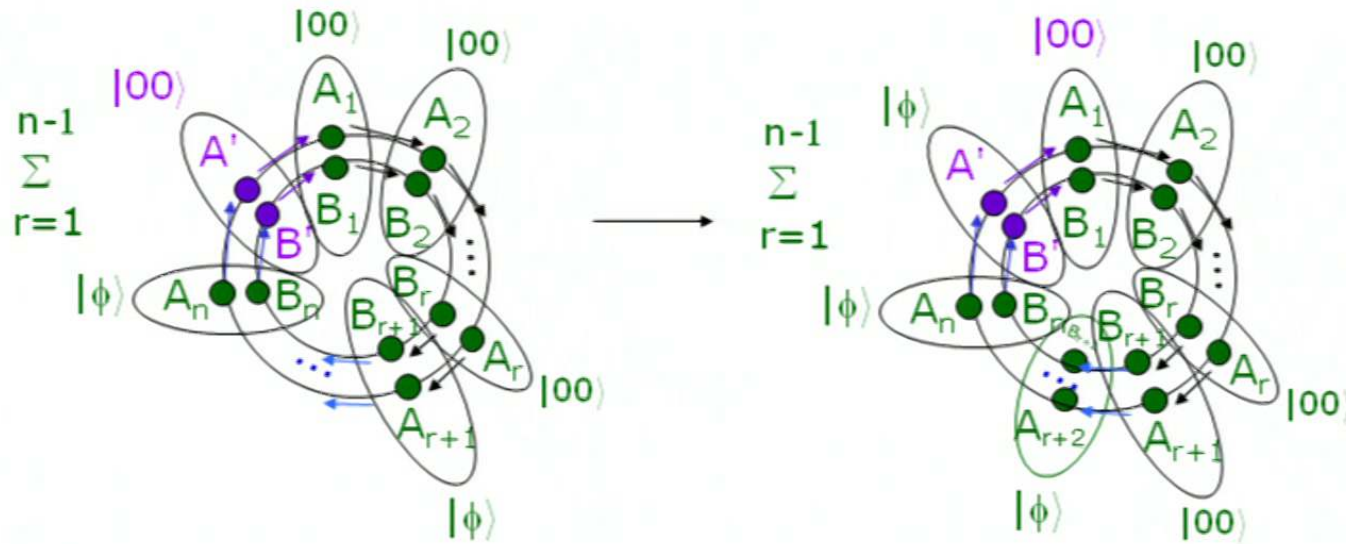
$$|00\rangle_{A'B'} \otimes |\psi\rangle_{AB}$$

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

Alternative (& obvious) embezzlement scheme

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

Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



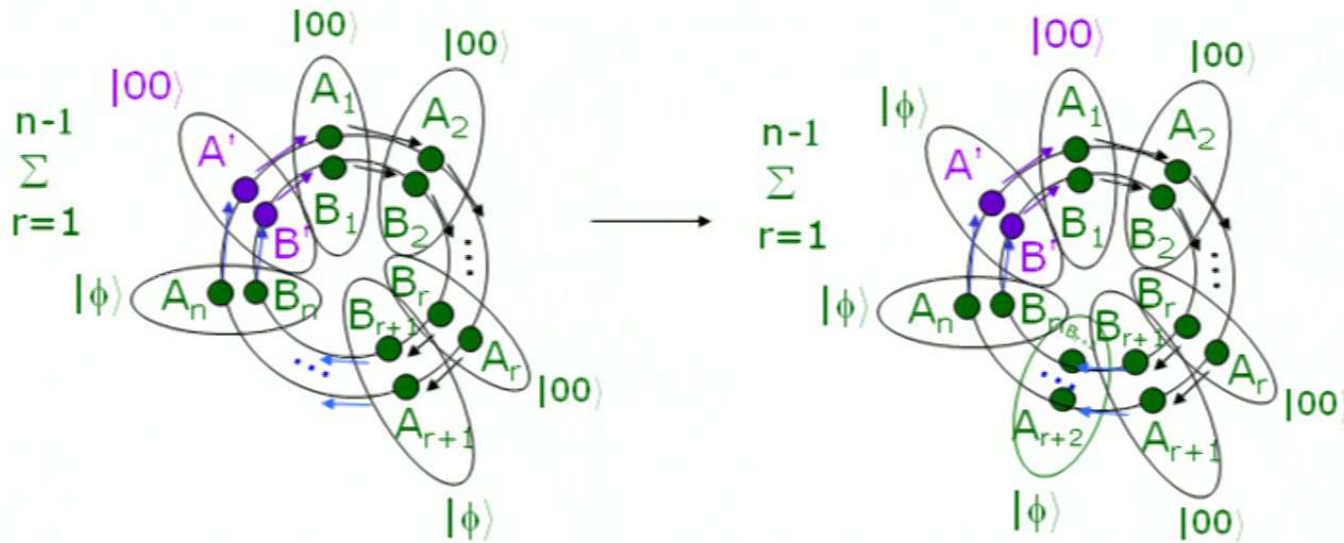
$$|00\rangle_{A'B'} \otimes |\psi\rangle_{AB} \longrightarrow |\phi\rangle_{A'B'} \otimes |\psi'\rangle_{AB}$$

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

Alternative (& obvious) embezzlement scheme

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

Choose: $A = A_1 \dots A_n, B = B_1 \dots B_n, \forall i, A_i \sim A', B_i \sim B'$



$$|00\rangle_{A'B'} \otimes |\psi\rangle_{AB}$$

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

→

$$|\phi\rangle_{A'B'} \otimes |\psi'\rangle_{AB} \approx^\epsilon |\psi\rangle_{AB} \text{ if } n = 1/\epsilon$$

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

Summary of the embezzlement scheme

$$\underbrace{|\psi\rangle_{AB} |00\rangle_{A'B'}}_{C \sum_{r=1}^{n-1} |00\rangle^{\otimes r} |\phi\rangle^{\otimes n-r}} \leftrightarrow \underbrace{|\psi'\rangle_{AB} |\phi\rangle_{A'B'}}_{C \sum_{r=2}^n |00\rangle^{\otimes r} |\phi\rangle^{\otimes n-r}} \approx^\varepsilon |\psi\rangle_{AB} |\phi\rangle_{A'B'}$$

- $\dim(AB) = \dim(A'B')^{(1/\varepsilon)}$ (close to optimal)
- works $\forall |\eta\rangle_{A'B'} \rightarrow |\phi\rangle_{A'B'}$ using $|\psi\rangle = C \sum_{r=1}^{n-1} |\eta\rangle^{\otimes r} |\phi\rangle^{\otimes n-r}$
- works for multiparty $|\eta\rangle$ & $|\phi\rangle$
- works for other reason why $|\eta\rangle \not\leftrightarrow |\phi\rangle$.

References for embezzlement:

- van Dam and Hayden, 0201041
- Leung, Toner and Watrous, 0804.4118
- Leung and Wang, 1311.6842

∞ -dim generalization, self-embezzlement:

- Haagerup, Scholz and Werner (in preparation)
- Cleve, Liu, Paulsen, 1606.05061
- Cleve, Collins, Liu, Paulsen, 1811.12575

Mismatched descriptions of what to embezzle:

- Steurer, Dinur, Vidick, 1310.4113
- Cleve, Lasecki, Leung (in preparation)

Open problems on embezzlement:

1. van Dam - Hayden scheme	LTW scheme
catalyst universal $\forall \phi\rangle$	catalyst depends on $ \phi\rangle$
unitaries depends on $ \phi\rangle$	unitaries independent of $ \phi\rangle$
bipartite states	multi-partite states

LTW scheme can use a universal catalyst: tensor product of catalysts for an ε -net of target states and a fixed initial state.

For embezzlement of multipartite state, is there a more efficient universal catalyst?

2. L, Wang 2013 showed that finite-dim embezzlement catalyst is essentially unique for bipartite setting. Same for multi-partite setting?

Outline:

1. Embezzlement
2. Approximate violation of conservation laws
& macroscopically controlled coherent operations
3. Finite Bell inequality that cannot be violated maximally
with finite amount of entanglement
4. Quantum reverse Shannon theorem

Local operations	→	Superselection rules
Entanglement	→	Conserved quantities (charge, spin etc)
Embezzlement	→	Generic recipe to approx an otherwise forbidden transformation

Suppose $|\eta\rangle \not\leftrightarrow |\phi\rangle$, say, because $|\eta\rangle$, $|\phi\rangle$ contain different amount of a *conserved* quantity.

Since cyclic permutation conserves the quantity, using

$|\psi\rangle = C \sum_{r=1}^{n-1} |\eta\rangle^{\otimes r} |\phi\rangle^{\otimes n-r}$ one can approx the transformation $|\psi\rangle|\eta\rangle \leftrightarrow^\varepsilon |\psi\rangle|\phi\rangle$ and "violate" the conservation law !

Furthermore, the approx transformation is **coherent**, and can be performed / not in superposition:

$$(a|0\rangle|\gamma\rangle + b|1\rangle|\eta\rangle) |\psi\rangle \leftrightarrow^{\varepsilon} (a|0\rangle|\gamma\rangle + b|1\rangle|\phi\rangle) |\psi\rangle$$

Thus $|\psi\rangle$ makes the superselection rule irrelevant.

Application: macroscopically-controlled gates

e.g., $|0\rangle_S$: spin down (ground state)

$|1\rangle_S$: spin up (excited state)

"X gate": $a|0\rangle_S + b|1\rangle_S \leftrightarrow a|1\rangle_S + b|0\rangle_S$ but $|0\rangle_S \not\leftrightarrow |1\rangle_S$

Allowed: $|r\rangle_L |0\rangle_S \leftrightarrow |r-1\rangle_L |1\rangle_S$

where $|k\rangle_L = k$ -photon state in laser beam.

But *changes in photon #* in laser beam decoheres the spin.

Solution: use $|\psi\rangle_L = \sum_{r=1}^{n-1} |r\rangle_L$:

$$|\psi\rangle_L (a|0\rangle_S + b|1\rangle_S) \leftrightarrow \underbrace{\sum_{r=1}^{n-1} |r-1\rangle_L}_{\approx |\psi\rangle_L} a|1\rangle_S + \underbrace{\sum_{r=1}^{n-1} |r+1\rangle_L}_{\approx |\psi\rangle_L} b|0\rangle_S$$

↙

$$\approx |\psi\rangle_L (a|1\rangle_S + b|0\rangle_S) \text{ nearly coherent X gate}$$

More on conservation laws

Kitaev, Mayers, & Preskill (0310088) investigated (in response to Popescu) if superselection rules (SSR) help quantum crypto by restricting adversarial behavior:

superposition of diff charges possible if a charge reservoir (a condensate \sim catalyst) is accessible, and SSR cannot enhance quantum cryptography.

Bartlett, Rudolph, and Spekkens generalized the "no-help" result, by connection to "reference frames" which are like the catalyst in this talk.

Embezzlement \rightarrow arbitrary unitary despite SSR (in progress)?
Latter solved by Popescu, Sainz, Short, and Winter
(1804.03730) (1-party, no embezzlement ...)

Caution for resource theories based on conservation laws ...

Outline:

1. Embezzlement
2. Approximate violation of conservation laws
& macroscopically controlled coherent operations
3. Finite Bell inequality that cannot be violated maximally
with finite amount of entanglement
4. Quantum reverse Shannon theorem

Embezzlement based **Bell inequality** that cannot be **violated maximally** with finite amount of entanglement

Embezzlement based **nonlocal game** that cannot be **played optimally** with finite amount of entanglement

Non-closure of quantum correlations via embezzlement

Joint work with Zhengfeng Ji & Thomas Vidick (1802.04926)

Nonlocal games

Referee

Player 1

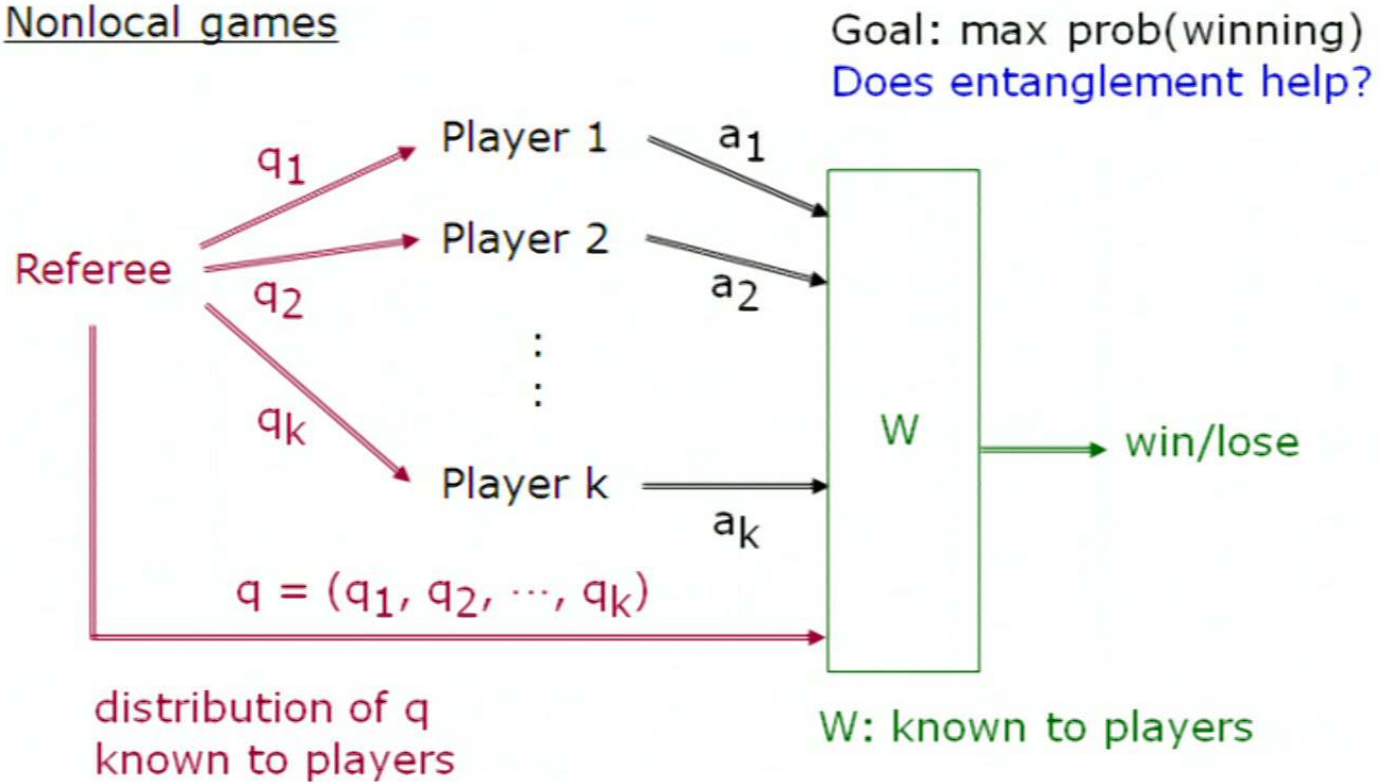
Player 2

⋮

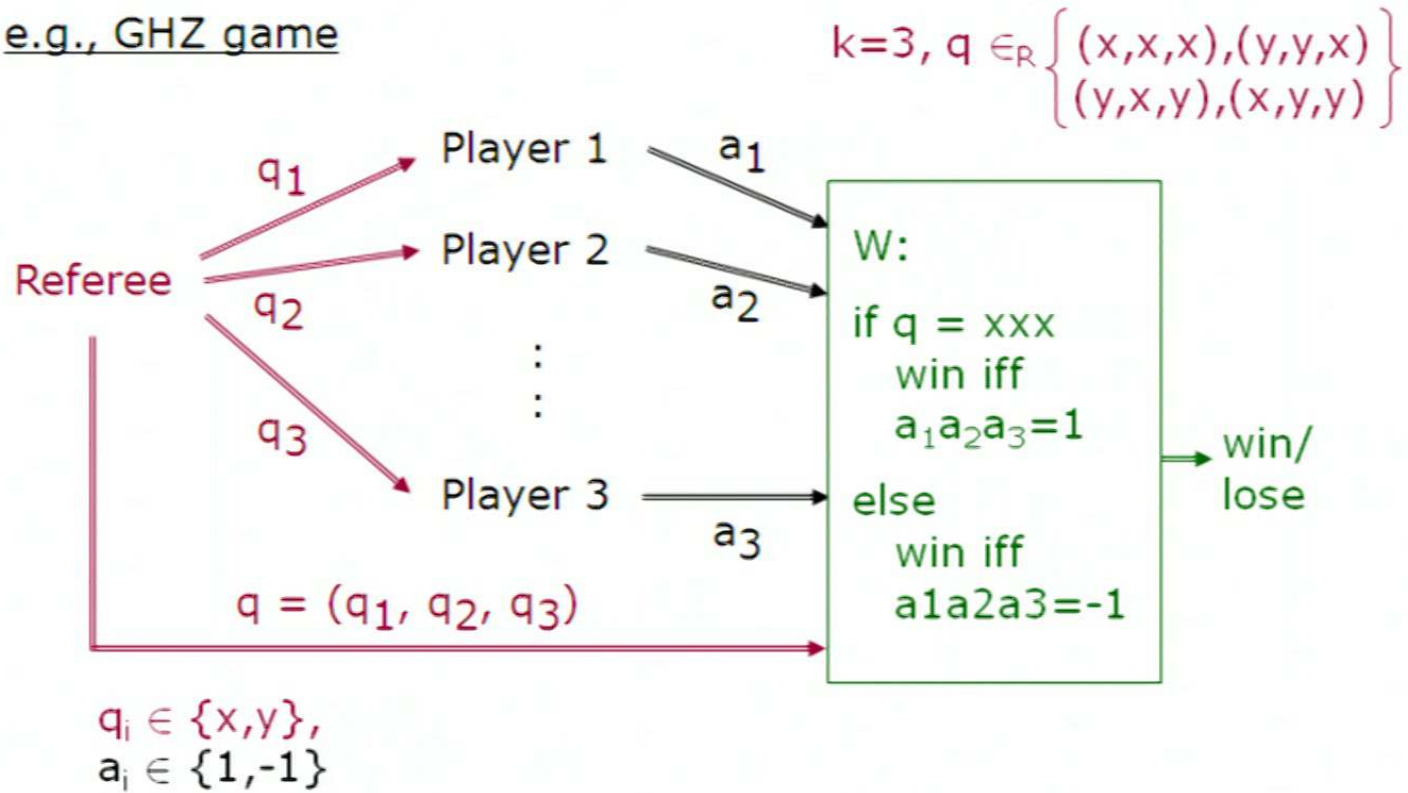
Player k

Players can coordinate before the game
noncommunicating once the game starts

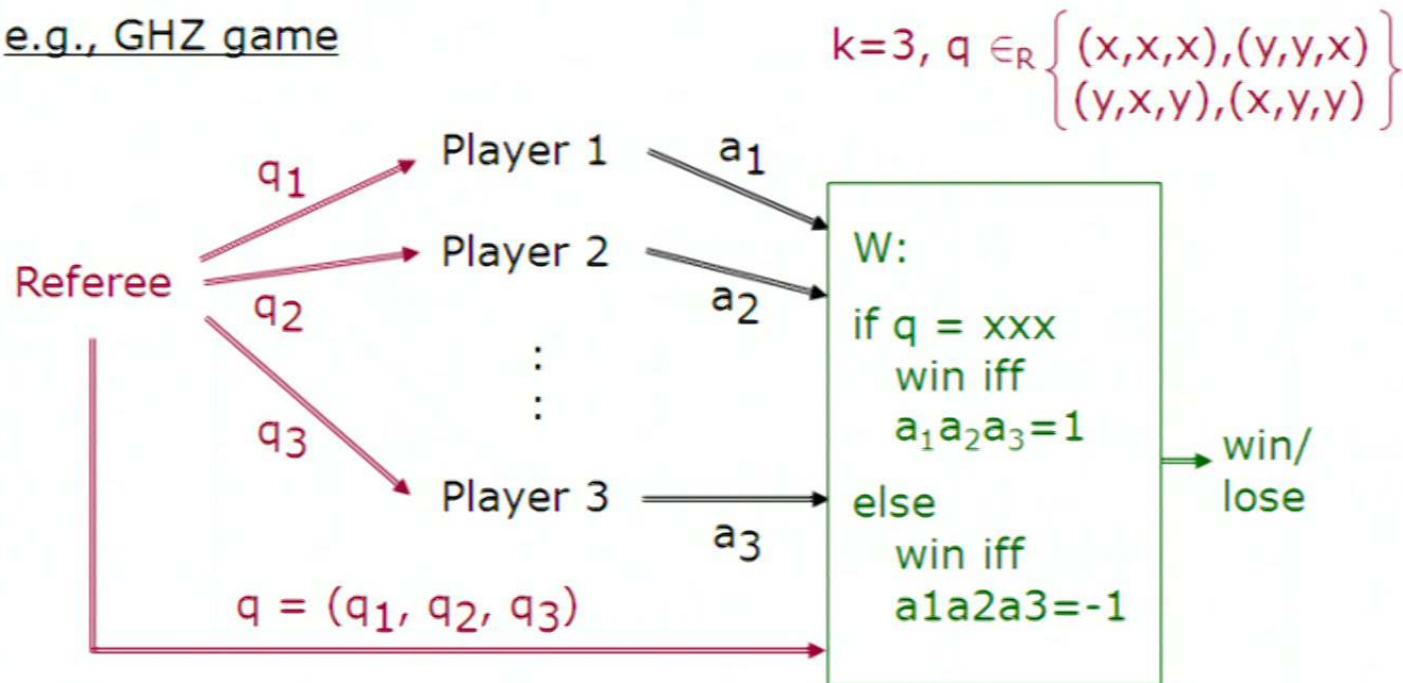
Nonlocal games



e.g., GHZ game



e.g., GHZ game



Without entanglement, winning prob $\leq 3/4$.

With a GHZ state, each party measures $\sigma_{x/y}$, winning prob = 1!

"Rigid" – unique optimal strategy (mod local isometries), robust.

Nonlocal games

Questions to players

Answers from players

Winning probability

Classical strategy

Bell experiments

Measurement settings

Measurement outcomes

Bell inequality

Local hidden variable model

shared randomness

Entangled strategy has
strictly higher winning
prob than classical

Violation of Bell inequality

Why nonlocal games?

Computational complexity -

Effects of entanglement in interactive proof systems

Physics -

QM vs local hidden variable model

Crypto -

QKD via rigidity (uniqueness of optimal solution)

Here: how much entanglement is needed to win optimally?

Conjecture since 2009: for some games with finitely many Q&A, more entanglement always strictly increases the winning prob.

Proofs:

Numerical evidence: Pal-Vertesi 09 (I3322)

Existential: Slofstra (+Vidick) 17, Dykema-Prakash-Paulsen 17

Here: how much entanglement is needed to win optimally?

Conjecture since 2009: for some games with finitely many Q&A, more entanglement always strictly increases the winning prob.

Proofs:

Numerical evidence: Pal-Vertesi 09 (I3322)

Existential: Slofstra (+Vidick) 17, Dykema-Prakash-Paulsen 17

Robust: dim lower bound vs deviation from optimal

Explicit: Ji, L, Vidick 18, Coladangelo-Stark 18, Coladangelo 19

JLV18: 3 parties, each with 12 questions and 8 or 4 answers
elementary proof + physical understanding

Turned a game from L, Toner, Watrous 08 into a nonlocal game.

LTW game has 2 parties, each with 3-dim quantum question
and 2-dim quantum answer, based on embezzlement.

The possibility & impossibility of embezzlement

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

Possibility of approximate embezzlement:

poor "continuity" of no-go thm

Poor continuity still limits how well one can embezzle

-- high accuracy requires more dim in the catalyst !

Limits to embezzlement of entanglement

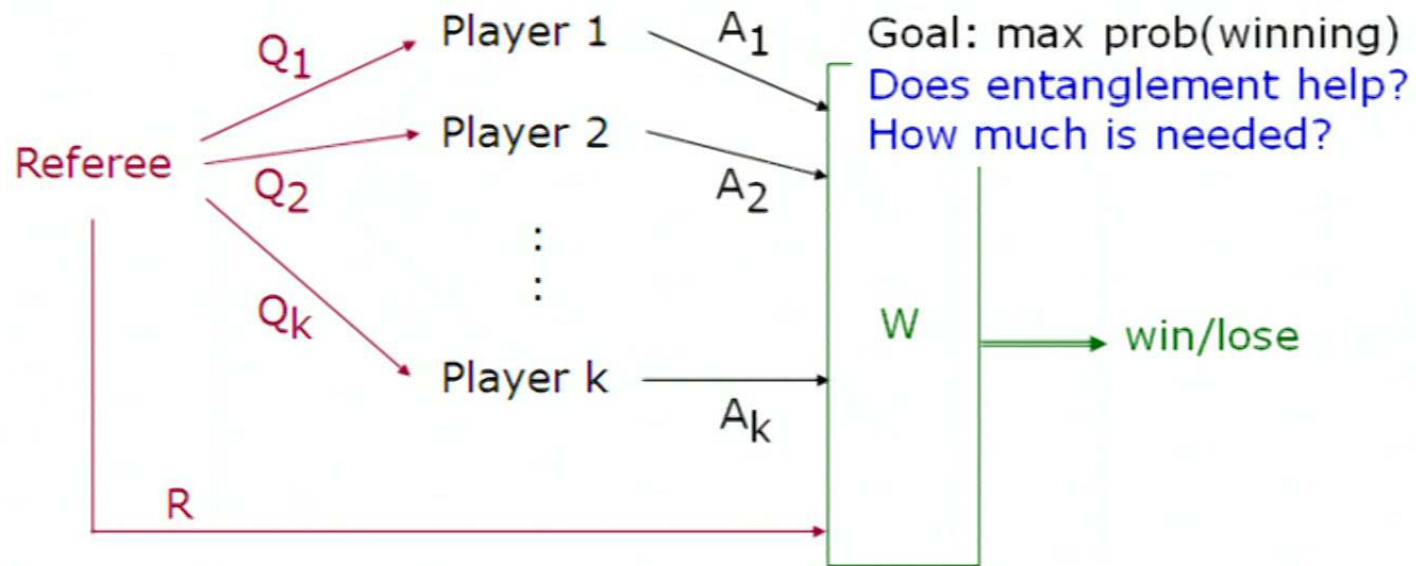
Theorem (from Fannes ineq):

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

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

"Nonlocal games" with quantum Qns & Ans



$Q_1, \dots, Q_k, A_1, \dots, A_k$: quantum sys

Initial state on R, Q_1, \dots, Q_k pure

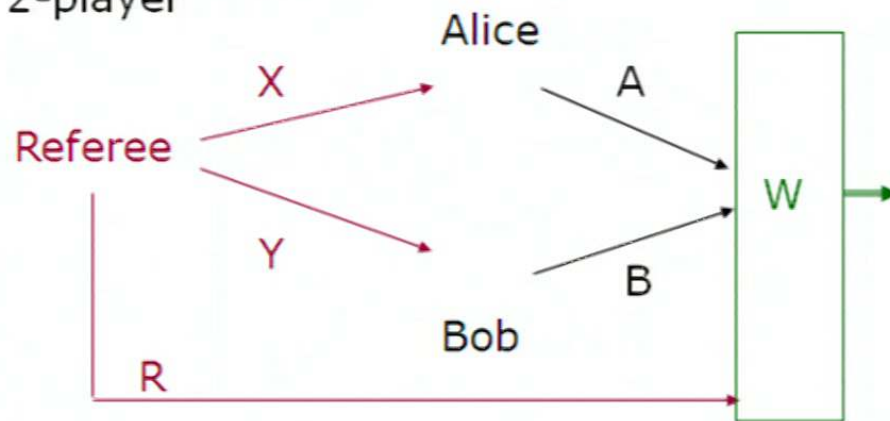
2-outcome POVM meas

known to players

Embezzlement game that cannot be won with finite entanglement

2-player

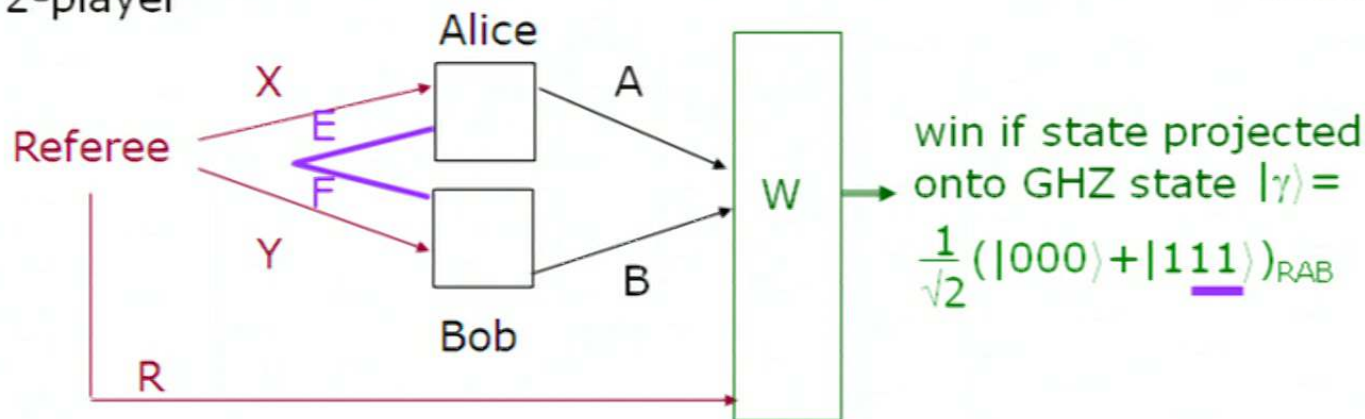
LTW08



Embezzlement game that cannot be won with finite entanglement

2-player

LTW08



Initial state on RXY:

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

Possible strategy:
 if X (Y) in $\text{span}\{|1\rangle, |2\rangle\}$
 then reverse-embezzle
 $|11\rangle + |22\rangle \rightarrow |11\rangle$.
 Winning prob $\rightarrow 1$.

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

Turning embezzlement game into a nonlocal game:

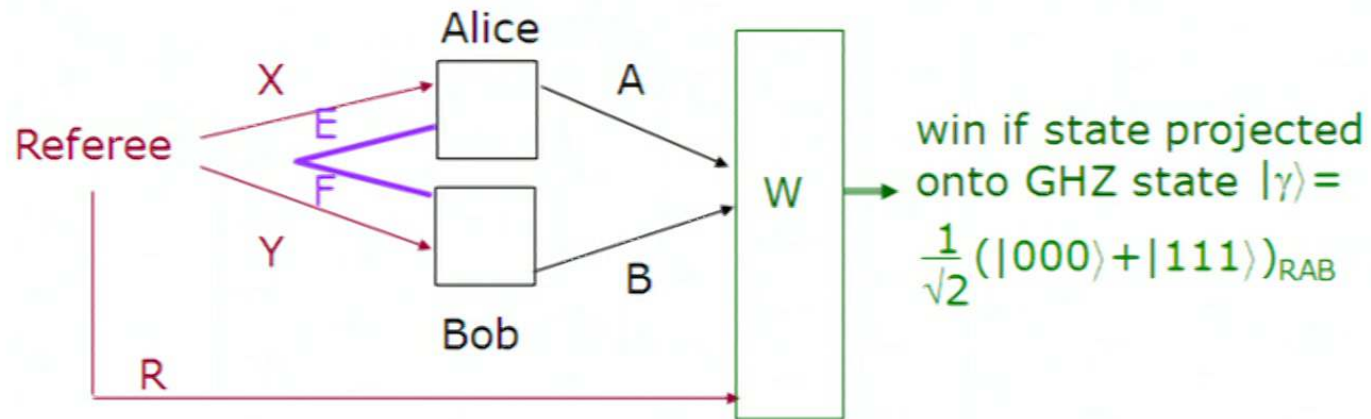
Regev and Vidick (1207.4939):

Referee's state R and answers AB classical

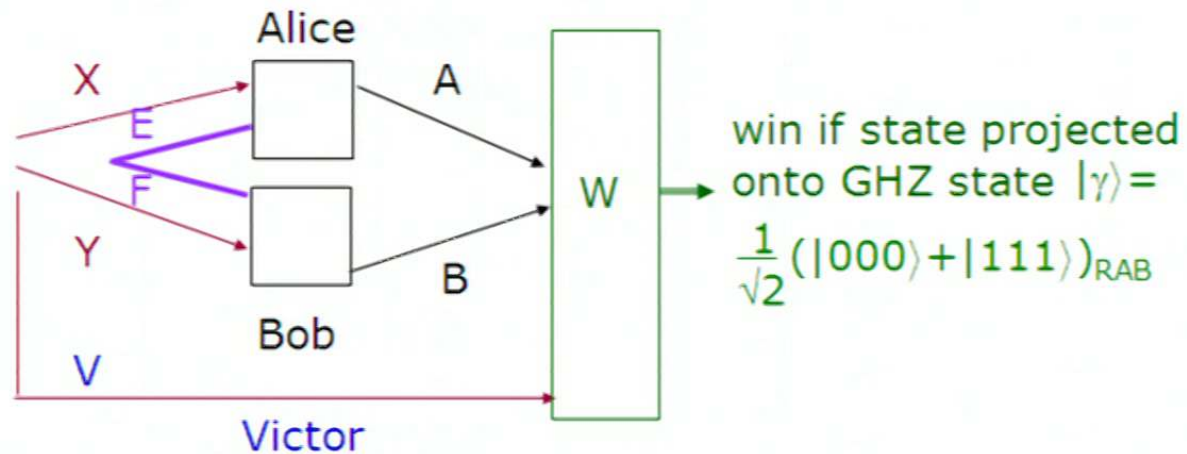
Questions XY remain quantum

Difficulty: distributing the initial state

Turning embezzlement game into a nonlocal game:

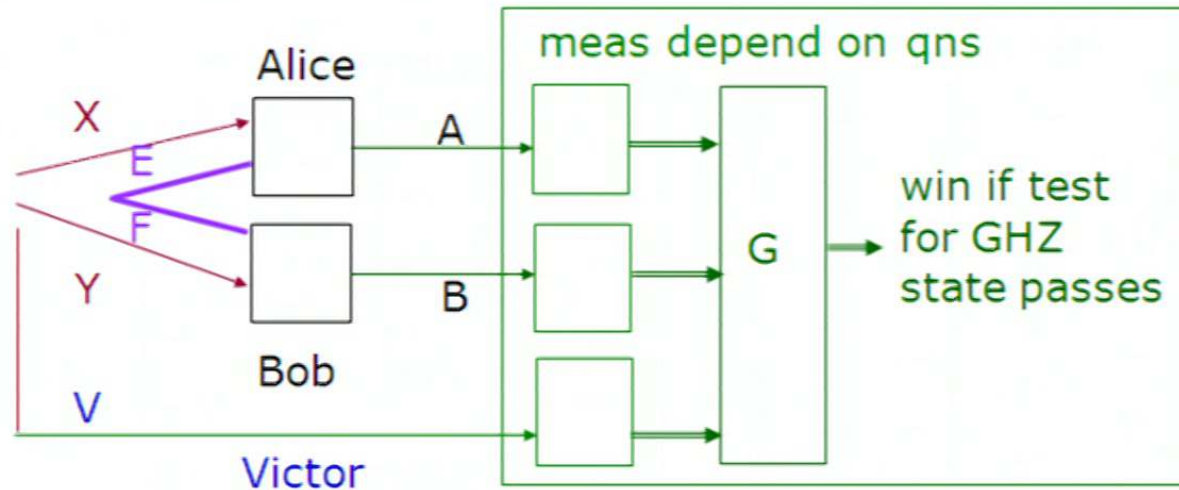


Turning embezzlement game into a nonlocal game (JLV18):



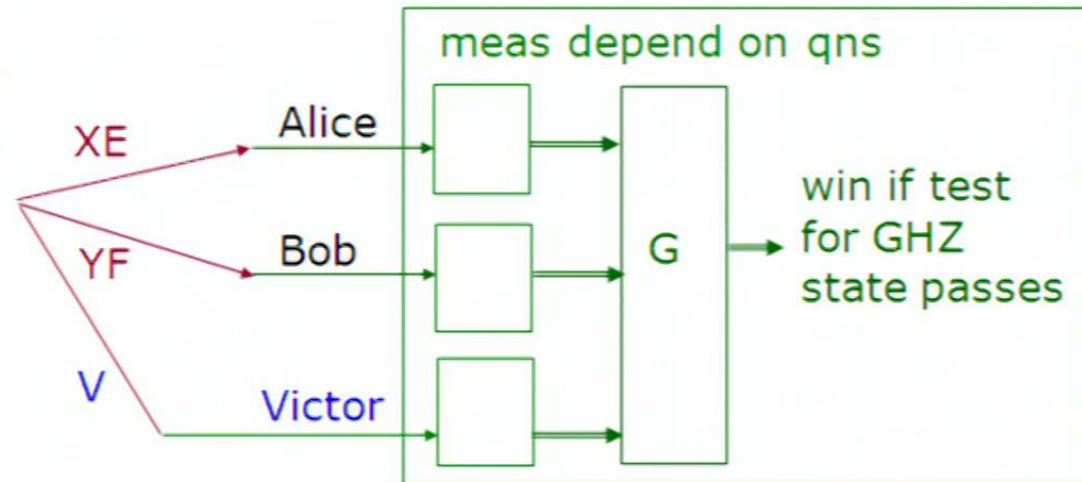
1. referee \rightarrow 3rd player Victor
initial state on XYR \rightarrow shared entanglement

Turning embezzlement game into a nonlocal game (JLV18):



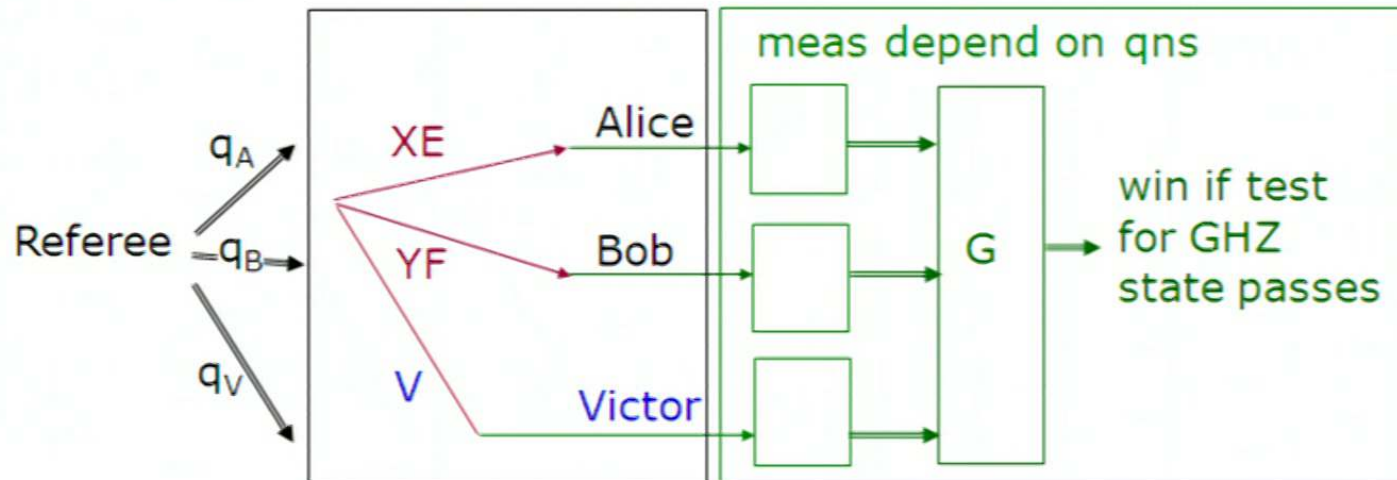
1. referee \rightarrow 3rd player Victor
initial state on $XYR \rightarrow$ shared entanglement
2. replace measurement by a rigidity test of the GHZ state

Turning embezzlement game into a nonlocal game (JLV18):



1. referee \rightarrow 3rd player Victor
initial state on XYR \rightarrow shared entanglement
2. replace measurement by a rigidity test of the GHZ state

Turning embezzlement game into a nonlocal game (JLV18):



1. referee \rightarrow 3rd player Victor
initial state on $XYR \rightarrow$ shared entanglement
2. replace measurement by a rigidity test of the GHZ state
3. Real referee R uses questions+winning conditions to enforce correct initial state & evolution.

Resulting game:

3-player, 12 questions each

3-bit answer from Victor, 2 bits from Alice & Bob each

1. **Suffices** for Victor, Alice, Bob to share entangled state with **3, $O(1/\epsilon)$, $O(1/\epsilon)$ qubits** to win $w_p > 1-\epsilon$.
2. **Necessary** for the entangled state to have at least **$\Omega(\epsilon^{-1/32})$ qubits** (exp that of Slofstra-Vidick-17).
3. Verification of increasing dim based on "1 test".

Open problems on nonlocal games & quantum games:

1. Is I3322 a game that will prove the conjecture in 2009?
2. Are there other physical reasons for requiring unbounded amount of entanglement to optimize Bell inequality violation?
3. The embezzlement (quantum) game shows: LU-assisted by entanglement is not a closed set for 3 input and 2 output dimensions? What is the minimum dimension for non-closure?
4. For LU-assisted by entanglement, if we allow approximations, is there a bound on the sufficient entanglement that depends only on the input/output dimensions?
5. For nonlocal games, is there a bound on entanglement independent of the game but depends only on the approximation and the number of questions and answers?
6. Applications of the embezzlement game or nonlocal game derived from it?

Outline:

1. Embezzlement
2. Approximate violation of conservation laws
& macroscopically controlled coherent operations
3. Finite Bell inequality that cannot be violated maximally
with finite amount of entanglement
4. Quantum reverse Shannon theorem