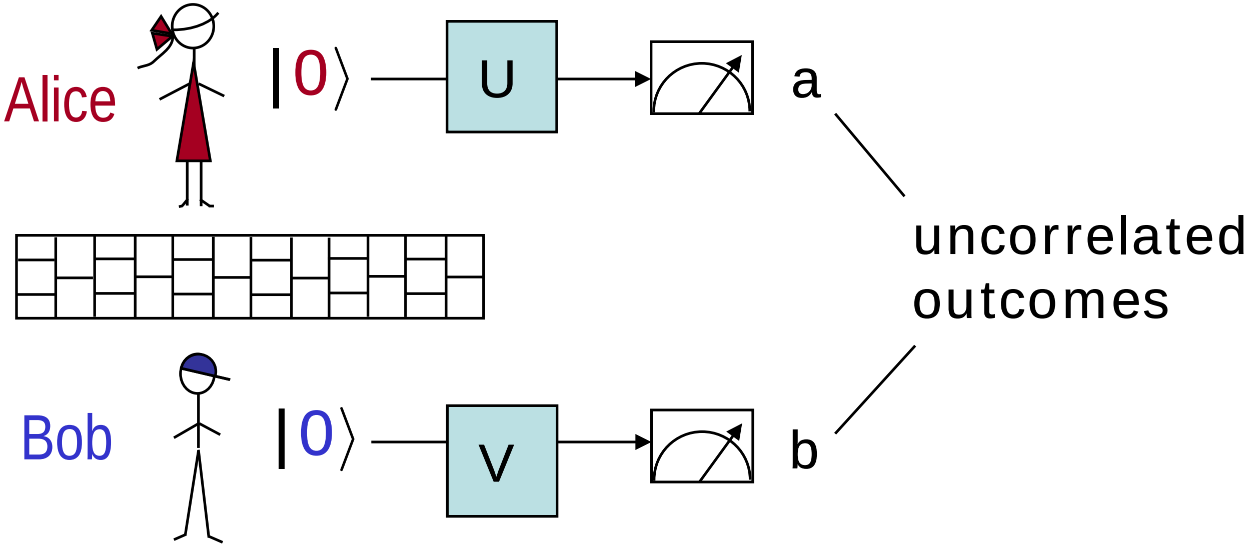
# Embezzlement and Applications

AQIS tutorial, August 19, 2019

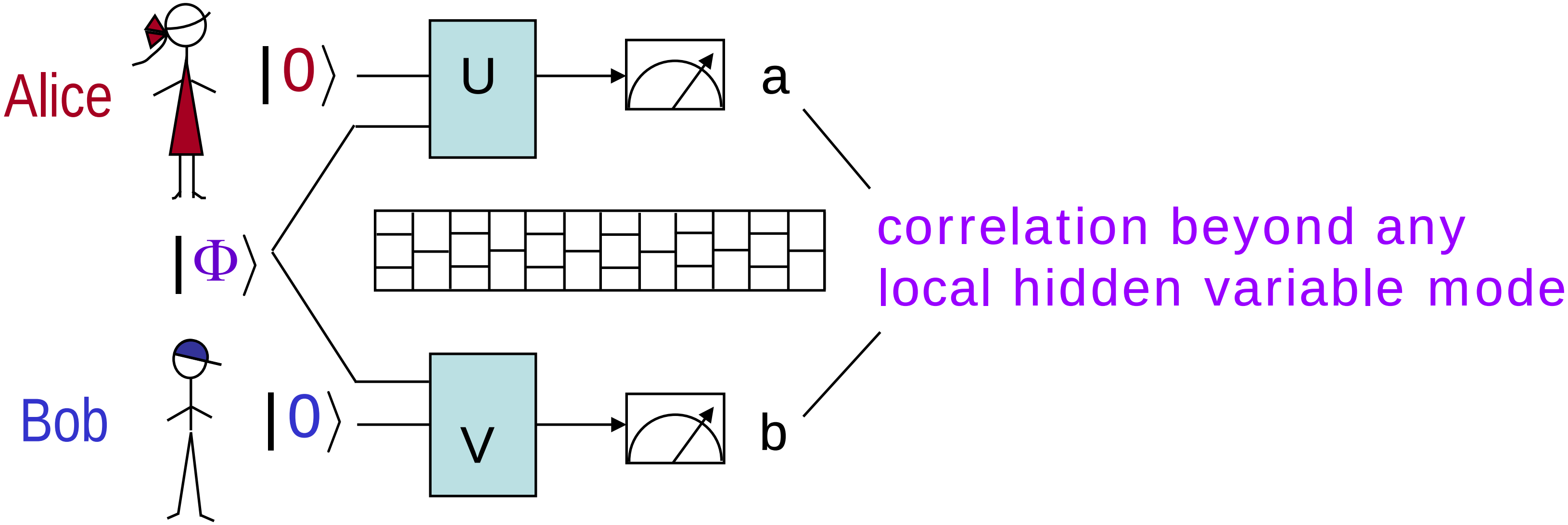
Debbie Leung

IQC and C&O, University of Waterloo
Perimeter Institute

# Local operations:

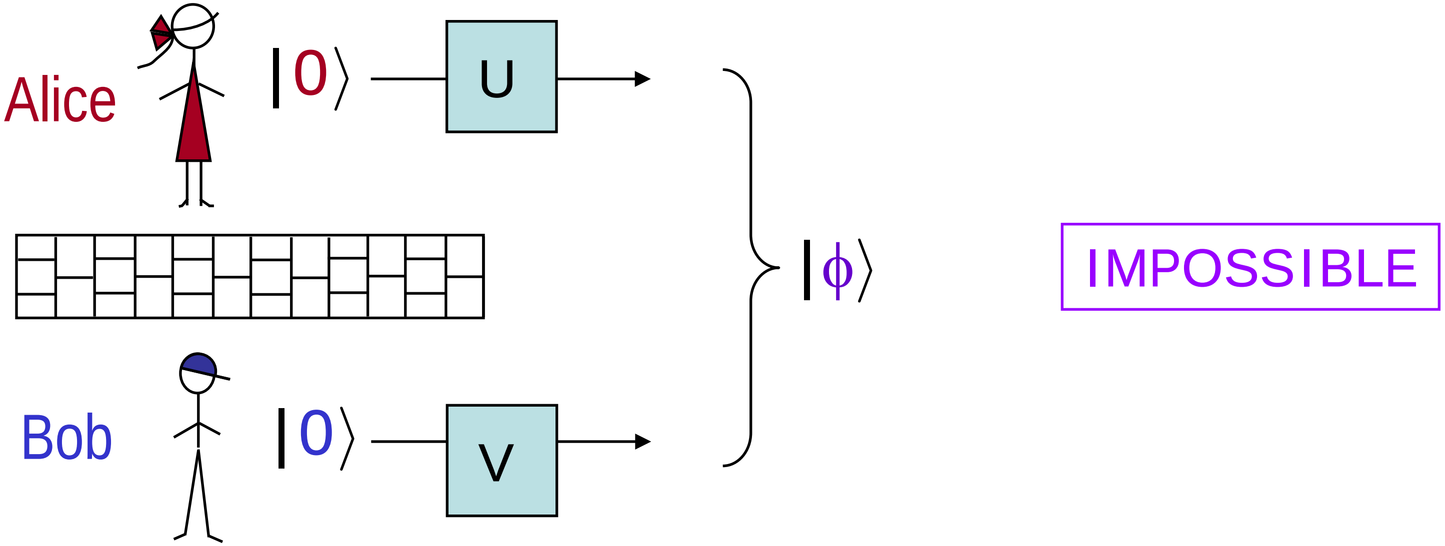


# Entanglement:

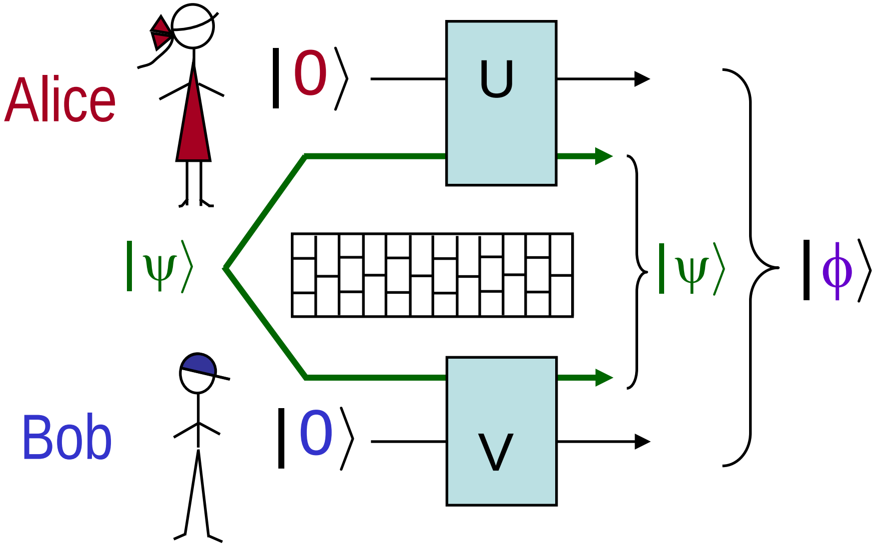



e.g., $|\Phi\rangle \propto |00\rangle + |11\rangle$

# No free entanglement:

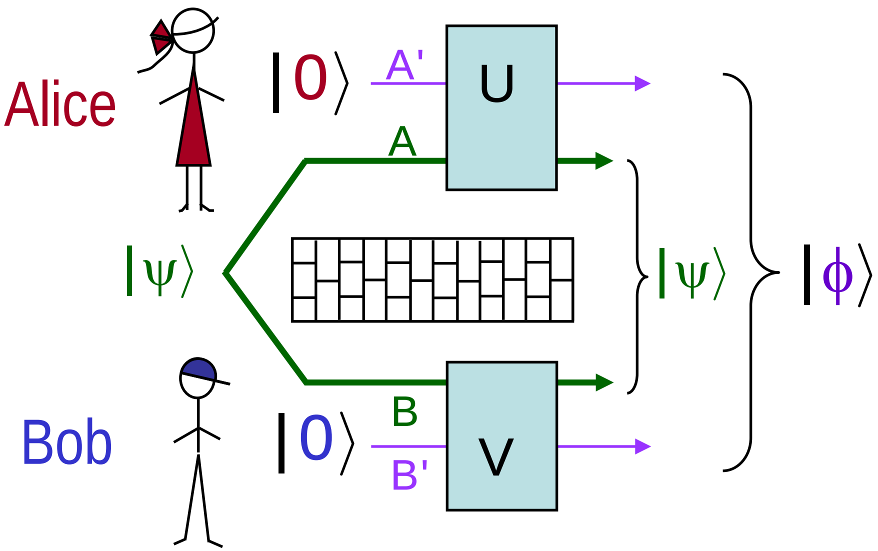


# No free entanglement even with a catalyst:




IMPOSSIBLE

# No free entanglement even with a catalyst:




IMPOSSIBLE

APPROX POSSIBLE

# Embezzlement of entanglement:

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

**Theorem.** $\forall\, \varepsilon > 0$, $\forall$ 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. $(U_{AA'} \otimes V_{BB'})\, |\psi\rangle_{AB}\, |00\rangle_{A'B'} \approx^{\varepsilon} |\psi\rangle_{AB}\, |\phi\rangle_{A'B'}$ !

van Dam & Hayden 2002

- conceived such possibility !
- one $|\psi\rangle$ (universal) fits all ($\forall$ 2-party $|\phi\rangle$ of fixed d)

$$|\psi\rangle \propto \sum_{k=1}^{N} (1/k)\, |k\rangle_A\, |k\rangle_B$$

## Embezzlement of entanglement:

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

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

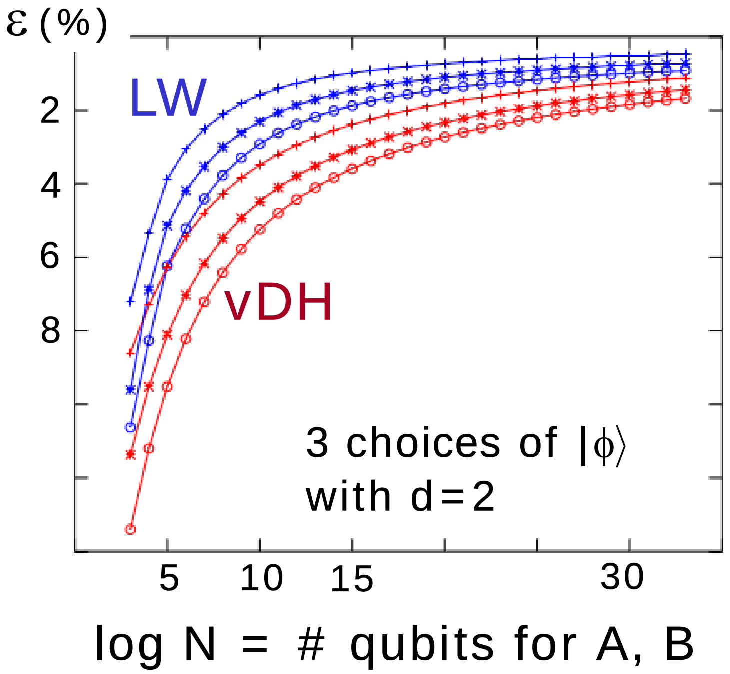
$\exists\, N$, $|\psi\rangle_{AB} \in C^N \otimes C^N$,

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

van Dam & Hayden 2002

- conceived such possibility !
- one $|\psi\rangle$ (universal)

  fits all ($\forall$ 2-party $|\phi\rangle$ of fixed d)




## Embezzlement of entanglement:

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

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

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

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

# Alternative (& obvious) embezzlement scheme

L, Toner, Watrous 08

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

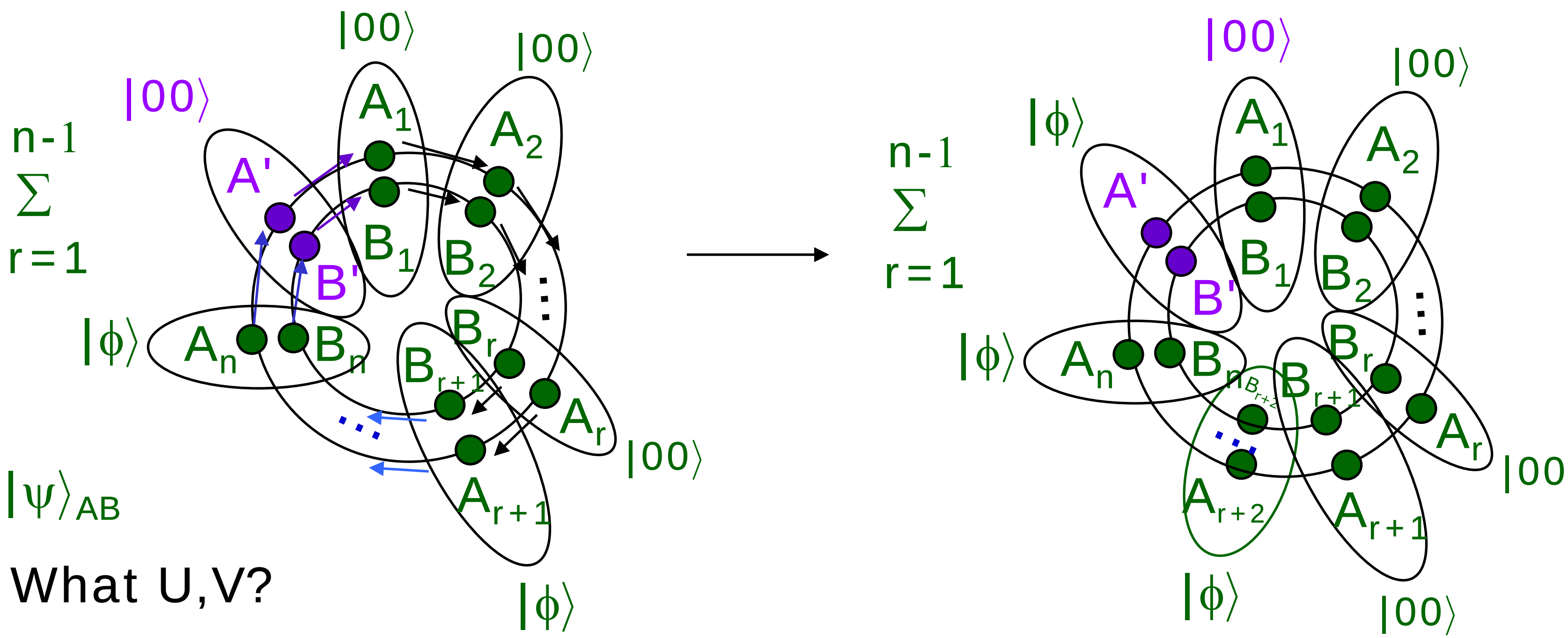
Given: A'B', $|\phi\rangle$

what AB, $|\psi\rangle$?

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




$$|00\rangle_{A'B'} \otimes |\psi\rangle_{AB} \longrightarrow |\phi\rangle_{A'B'} \otimes \boxed{|\psi'\rangle_{AB} \approx^{\varepsilon} |\psi\rangle_{AB} \text{ if } n = 1/\varepsilon}$$

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

# Summary of the embezzlement scheme

$$|\psi\rangle_{AB}\,|00\rangle_{A'B'} \quad \leftrightarrow \quad |\psi'\rangle_{AB}\,|\phi\rangle_{A'B'} \;\approx^{\varepsilon}\; |\psi\rangle_{AB}\,|\phi\rangle_{A'B'}$$

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

- $\dim(AB) = \dim(A'B')^{(1/\varepsilon)}$ (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 multipartite $|\eta\rangle$ & $|\phi\rangle$
- 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
- Connes and Stormer, J functional analysis 28, 187 (1978)

$\infty$-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

## 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 $\varepsilon$-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 universal embezzlement in the 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)

SSR: Restricted Hamiltonian or unitary that are block-diagonal

"Block index" is conserved

Local operations $\longrightarrow$ Superselection rules

Entanglement $\longrightarrow$ Conserved quantities (charge, spin etc)

Embezzlement $\longrightarrow$ 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.

Cyclic permutation conserves the quantity (allowed).

Using $|\psi\rangle = C \sum_{r=1}^{n-1} |\eta\rangle^{\otimes r} |\phi\rangle^{\otimes n-r}$ one can perform

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

$$\rightarrow C \sum_{r=1}^{n-1} |\eta\rangle^{\otimes r+1} |\phi\rangle^{\otimes n-r-1} |\phi\rangle \approx^{\varepsilon} |\psi\rangle|\phi\rangle$$

and "violate" the conservation law !

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

Conditioned on 1st register being $|1\rangle$ , apply $|\psi\rangle|\eta\rangle \to^{\varepsilon} |\psi\rangle|\phi\rangle$

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

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

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

$\rightarrow\ \approx |\psi\rangle_L\,(a|1\rangle_S + b|0\rangle_S)$ nearly coherent X gate

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

$|\psi\rangle_L\,(a|0\rangle_S + b|1\rangle_S) \leftrightarrow \approx |\psi\rangle_L\,(a|1\rangle_S + b|0\rangle_S)$

In the lab, we use the coherent state $|\psi\rangle_L \propto \sum_{r=1}^{n-1} \alpha^r / \sqrt{(r!)}\,|r\rangle_L$ !

Local operations → Superselection rules

Entanglement → Conserved quantities (charge, spin etc)

Embezzlement → Generic recipe to approx an otherwise forbidden transformation

Principle: use catalyst to introduce a large uncertainty of the conserved quantity to enable approximately violation of conservation law

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

Uncertainty in # of copies of $|00\rangle$ vs $|\phi\rangle$

$|\psi\rangle_L \propto \sum_{r=1}^{n-1} |r\rangle_L$

Uncertainty in photon #

# 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 ~ catalyst) is accessible, and SSR cannot enhance quantum cryptography.

Bartlett, Rudolph, and Spekkens (0610030) generalized the above, by connection to "reference frames" which are like the catalyst in this talk.

Embezzlement $\rightarrow$ arbitrary unitary despite SSR ?

Latter solved by Popescu, Sainz, Short, Winter (1804.03730)

1-party result, does not give embezzlement ...

## 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

References:


- Leung, Toner, Watrous (0804.4118)
- Ji, Leung, Vidick (1802.04926)
- Coladangelo (1904.02350)

# Nonlocal games

Player 1

Player 2

Referee

:

:

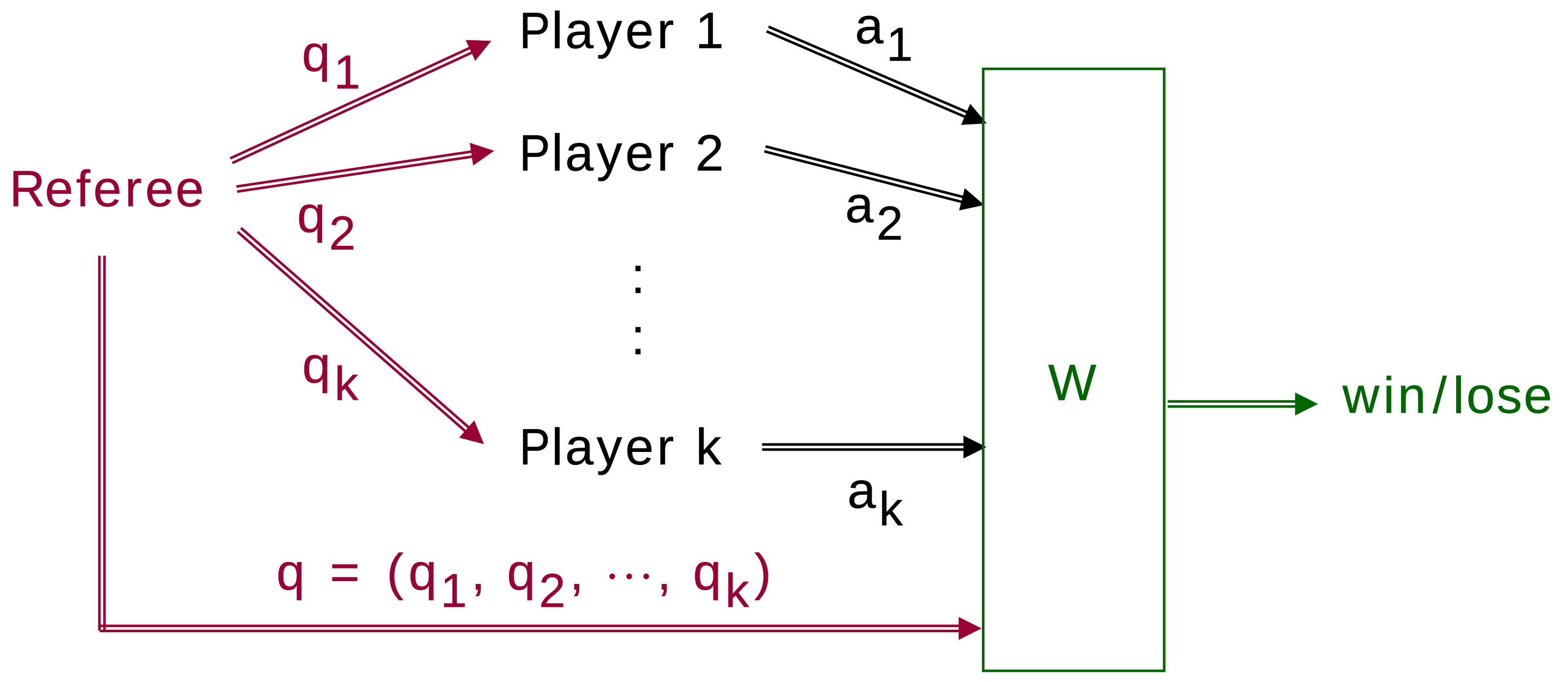
Player k

Players can coordinate before the game
noncommunicating once the game starts

Nonlocal games

Goal: max prob(winning)

Does entanglement help?

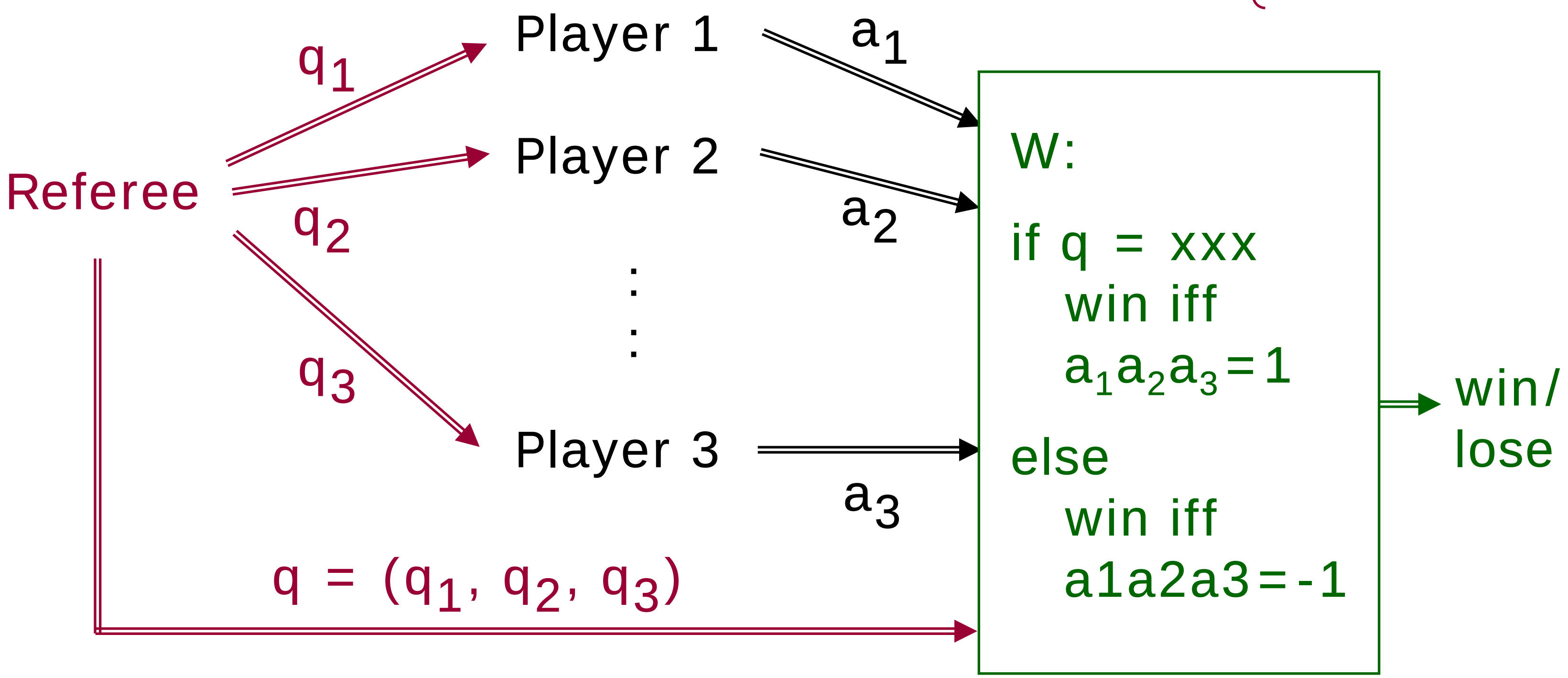



distribution of q
known to players

W: known to players

## e.g., GHZ game

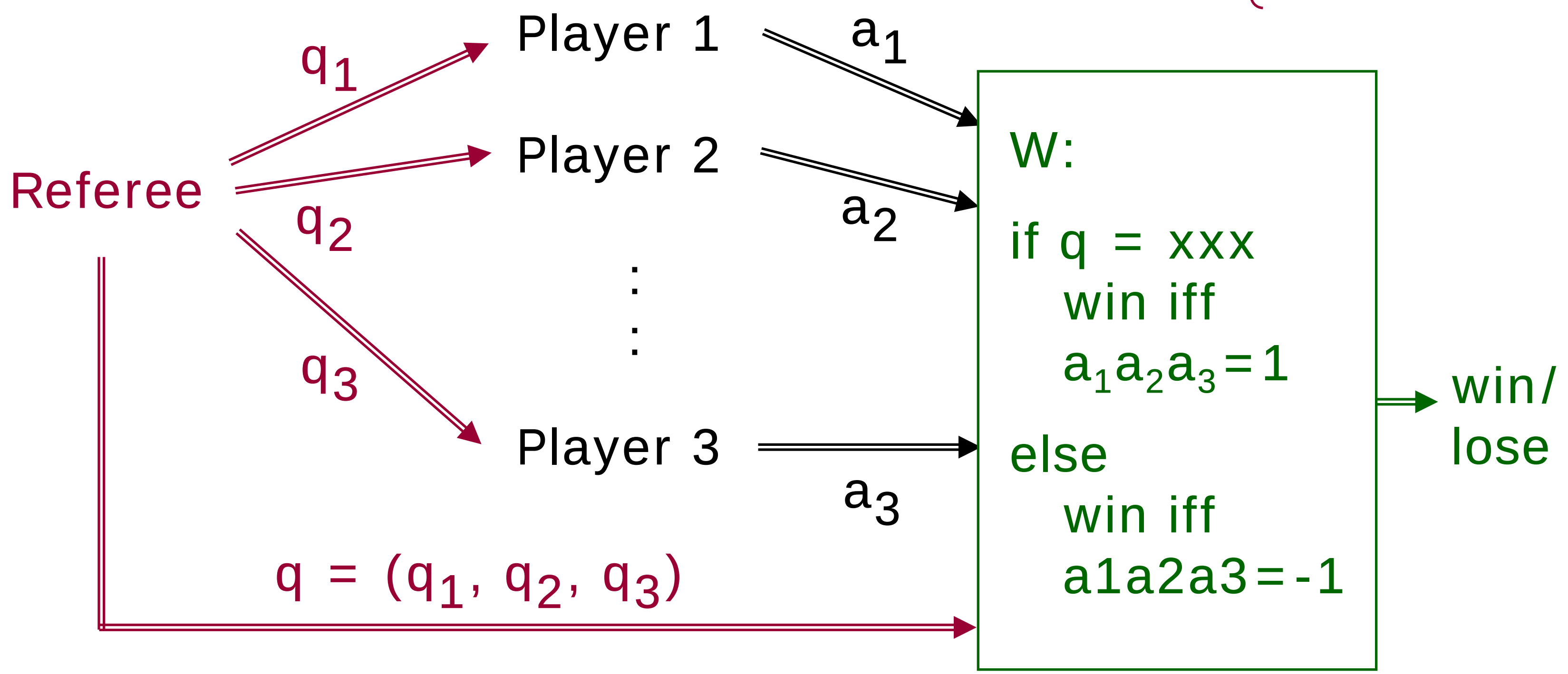
$k=3,\ q \in_R \left\{ \begin{matrix} (x,x,x),(y,y,x) \\ (y,x,y),(x,y,y) \end{matrix} \right\}$




$q_i \in \{x,y\}$,
$a_i \in \{1,-1\}$

e.g., GHZ game

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




Without entanglement, winning prob $\leq$ ¾ .

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

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

| Nonlocal games | Bell experiments |
| --- | --- |
| Questions to players | Measurement settings |
| Answers from players | Measurement outcomes |
| Prob(win) $\rightarrow$ payoff function | Bell inequality |
| Classical strategy | 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

Robust: dim lower bound vs deviation from optimal

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

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, C19 (elementary proof + physical understanding
+ exponentially stronger dim bound):

Turn a game from L, Toner, Watrous 08 into nonlocal games
LTW game has 2 parties, each with 3-dim quantum question and 2-dim quantum answer, based on embezzlement.

JLV18: 3 parties, each with 12 questions and 8 or 4 answers
C19: 2 parties, 5 or 6 questions and 3 answers each

## The possibility & impossibility of embezzlement

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

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

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

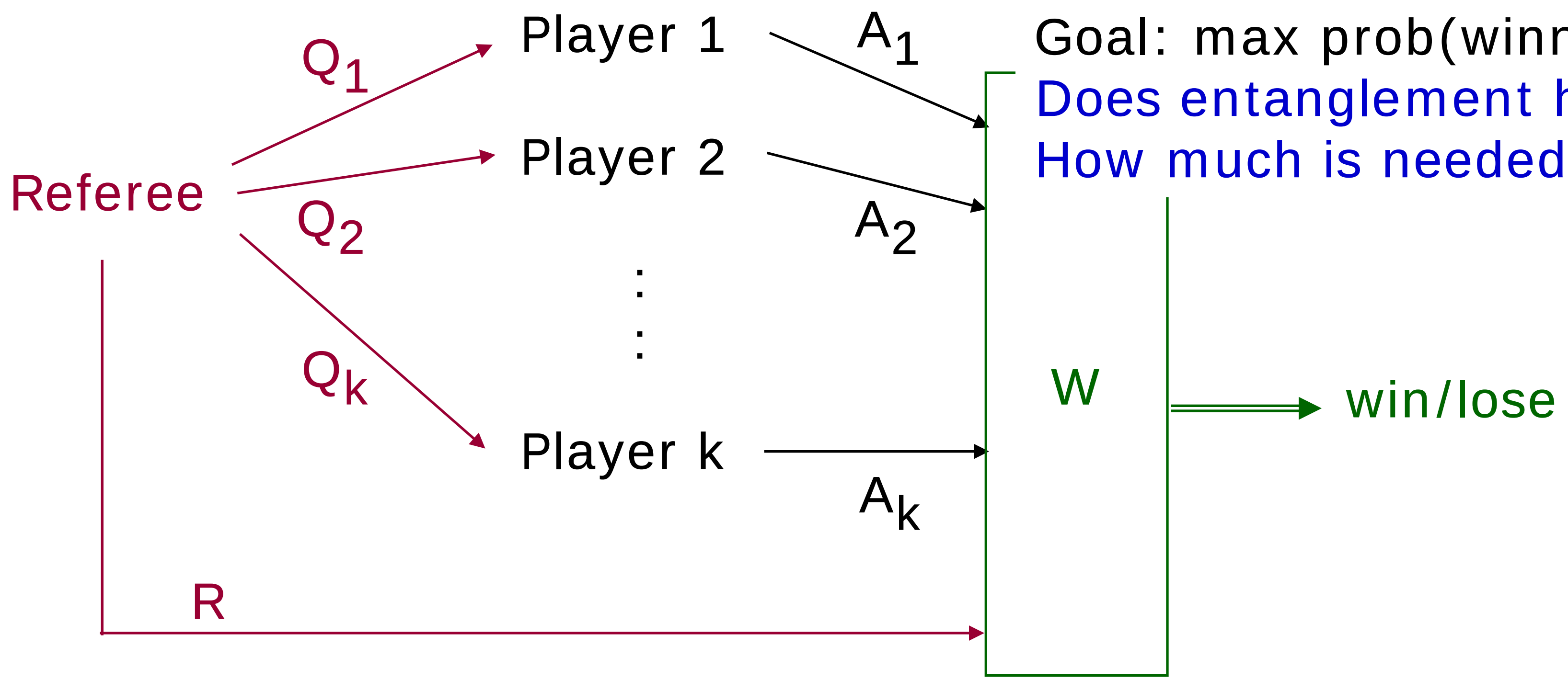
then $\varepsilon \geq 8\,[\,E(|\phi\rangle)\,/\,(\log N + \log d)\,]^2$

# "Nonlocal games" with quantum Qns & Ans

Goal: max prob(winning)

Does entanglement help?

How much is needed?




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

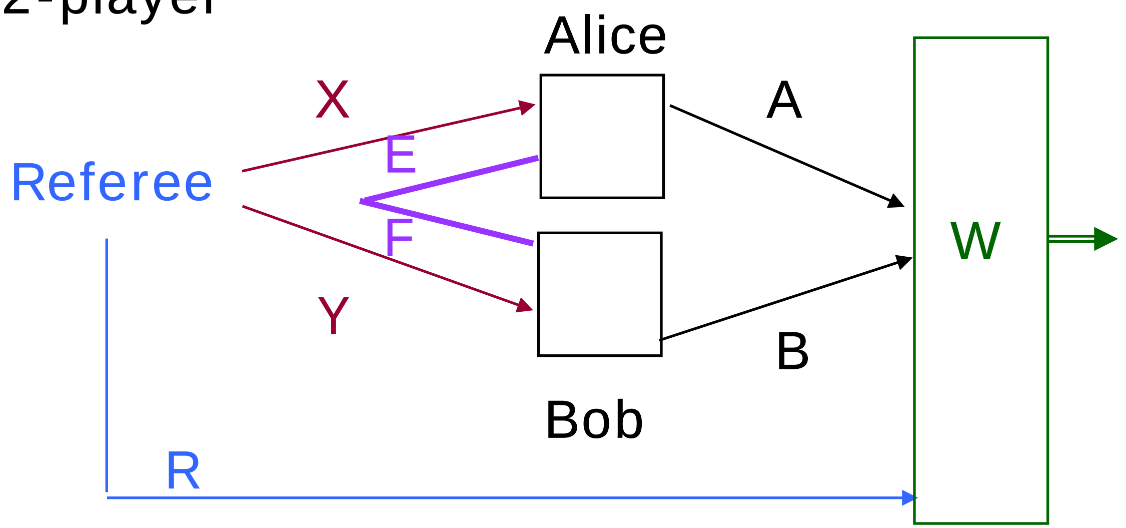
Initial state on R $Q_1, \cdots, Q_k$ pure — 2-outcome POVM meas

known to players

# Embezzlement game that cannot be won with finite entanglement

LTW08

2-player




win if state projected onto GHZ state $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{RAB}$

Initial state on RXY:

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

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

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

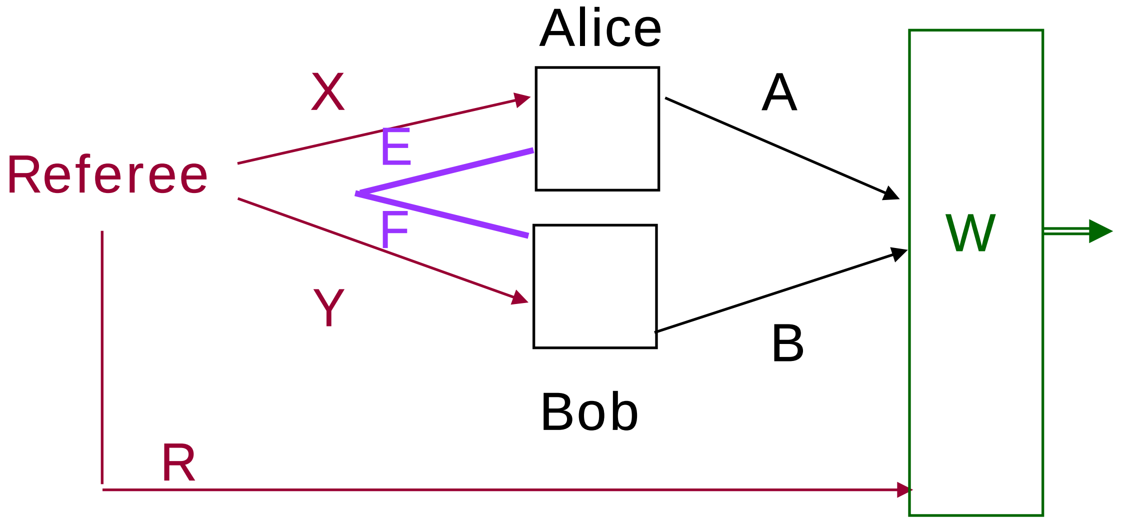
## Turning embezzlement game into a nonlocal game:

Regev and Vidick (1207.4939):

Referee's state R and answers AB classical
Questions XY remain quantum

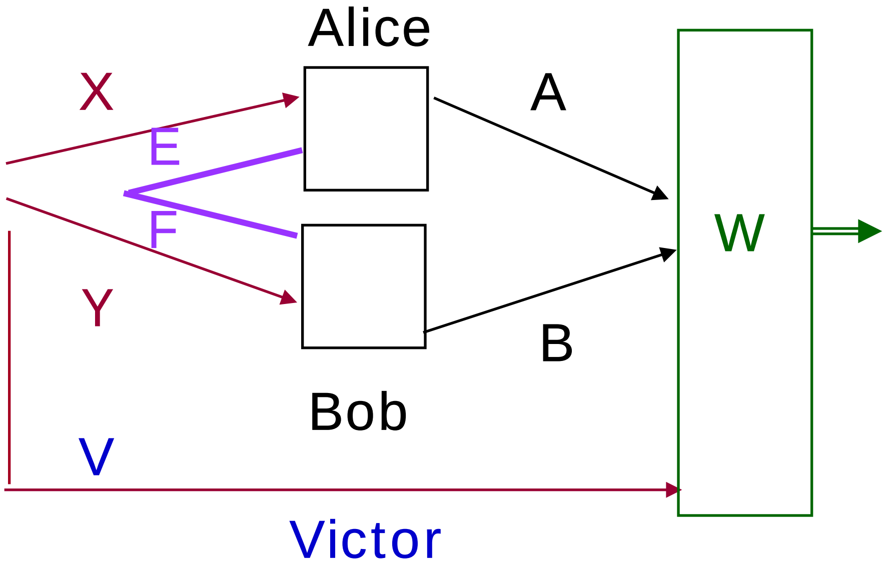
Difficulty: distributing the initial state

## Turning embezzlement game into a nonlocal game:




win if state projected onto GHZ state $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{RAB}$

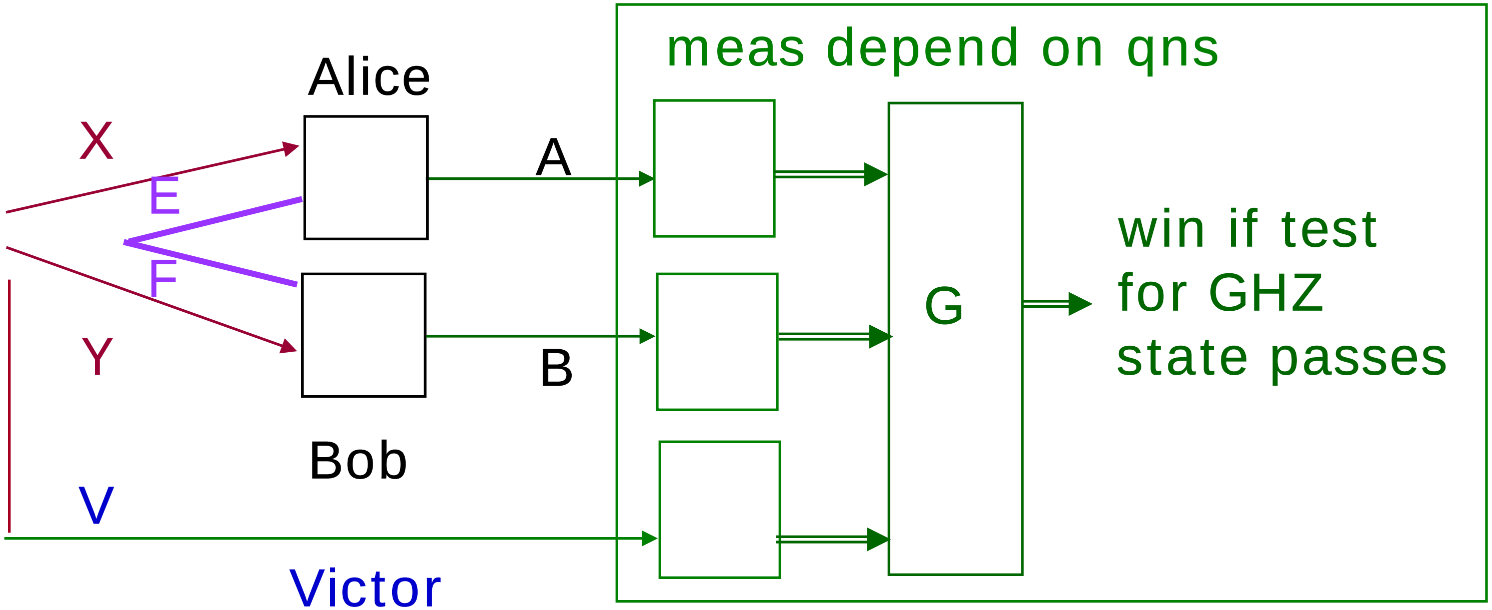
# Turning embezzlement game into a nonlocal game (JLV18):




win if state projected onto GHZ state $|\gamma\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{RAB}$

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

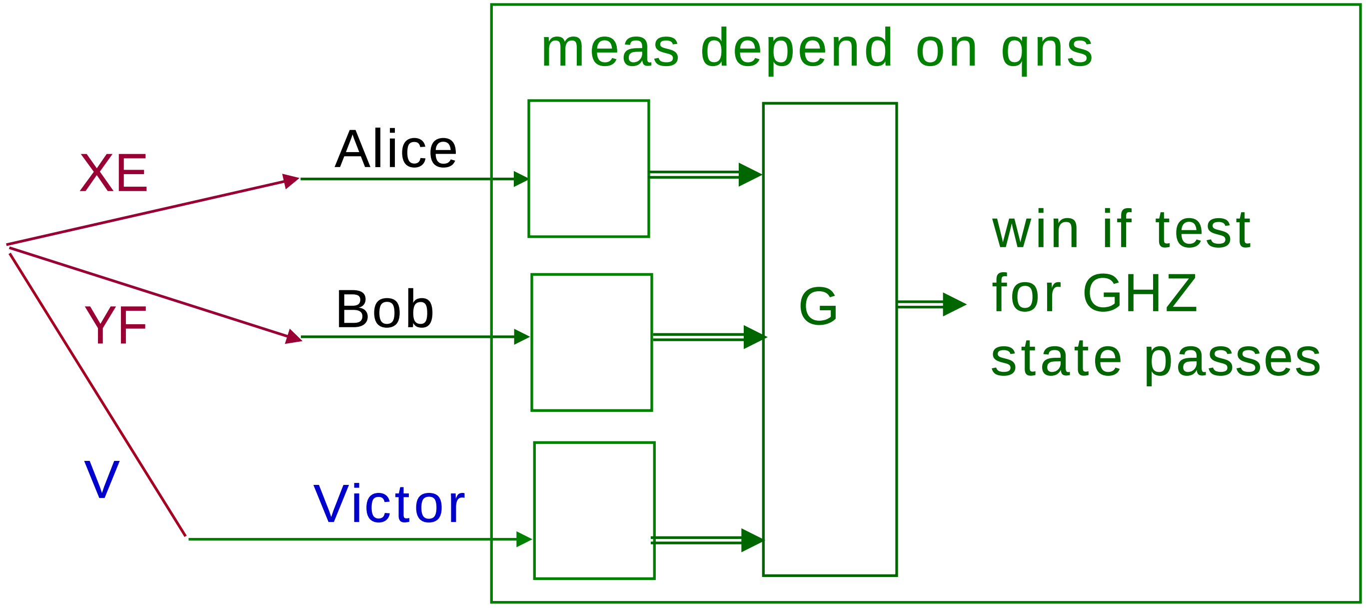
Turning embezzlement game into a nonlocal game (JLV18):




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

2. replace measurement by a rigidity test of the GHZ state

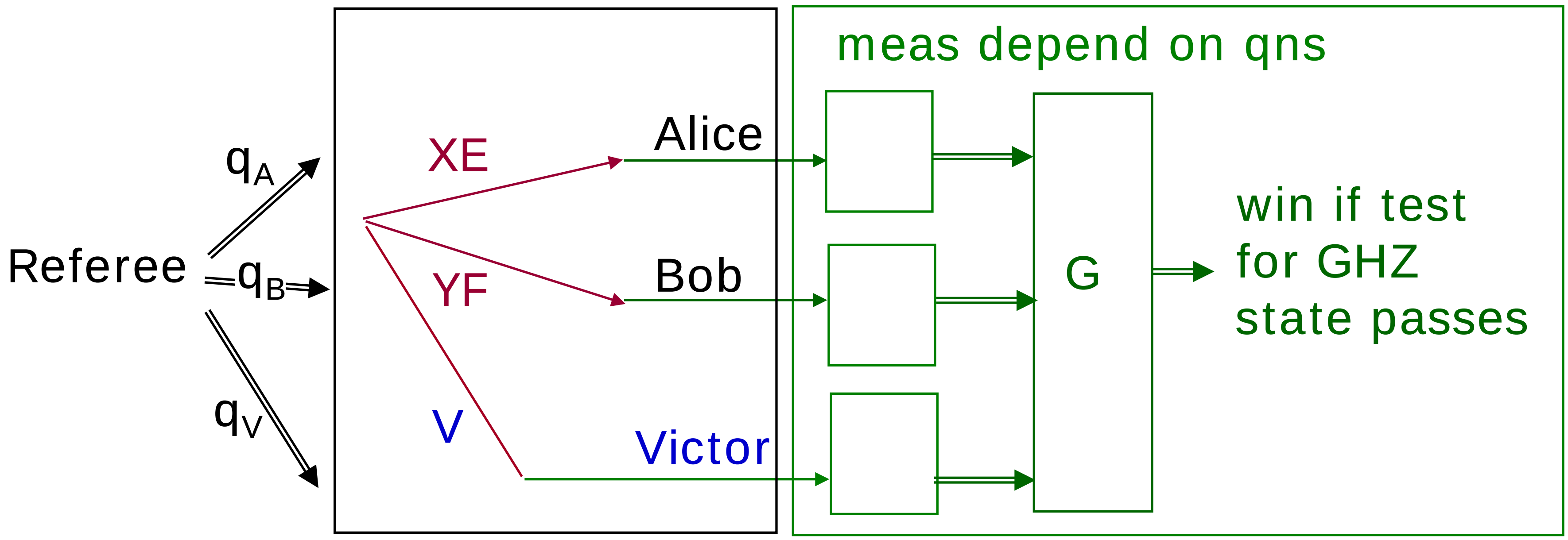
# Turning embezzlement game into a nonlocal game (JLV18):




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, $O(1/\varepsilon)$, $O(1/\varepsilon)$ qubits to win wp > $1-\varepsilon$.

2. Necessary for the entangled state to have at least
   $\Omega(\varepsilon^{-1/32})$ qubits (exp that of Slofstra-Vidick-17).

3. Verification of increasing dim based on "1 test".

## Turning embezzlement game into a nonlocal game (C19):

Goal: forcing the players to convert $\frac{(|11\rangle + |22\rangle)}{\sqrt{2}}$ into $|11\rangle$

Referee conducts one of 3 possible games $G_1$, $G_2$, $G_3$:

$G_1$ can only be won close-to-optimally with a state close to

$$\frac{|00\rangle + |11\rangle + |22\rangle}{\sqrt{3}}$$

$G_2$ can only be won close-to-optimally with a state close to

$$\frac{|00\rangle + \sqrt{2}|11\rangle}{\sqrt{3}}$$

$G_3$ ensures that the states above live in the same Hilbert space!

## Open problems on nonlocal games & quantum games:

1. Is I3322 a game that will proof the conjecture in 2009?
2. Are there other physical reasons for requiring unbounded amount of entanglement to optimize Bell ineq 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 min dim 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 dims?
5. For nonlocal games, is there a bound on entanglement independent of the game but depends only on the approx and the # qns and ans?
6. Applications of the embezzlement game or nonlocal game derived from it? e.g., JLV18, C19 games verify increasing dims.

## Outline:

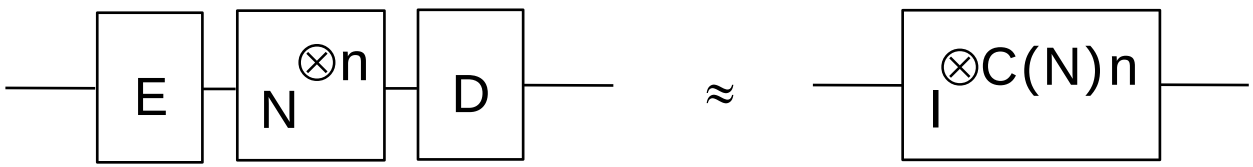
1. Embezzlement
2. Approximate violation of conservation laws
   & macroscopically controlled coherent operations
3. Finite Bell inequality that cannot be violated maximally
   with finite amount of entanglement
4. Quantum reverse Shannon theorem

# <u>Quantum reverse Shannon theorem:</u>

Quantum Shannon theorem:

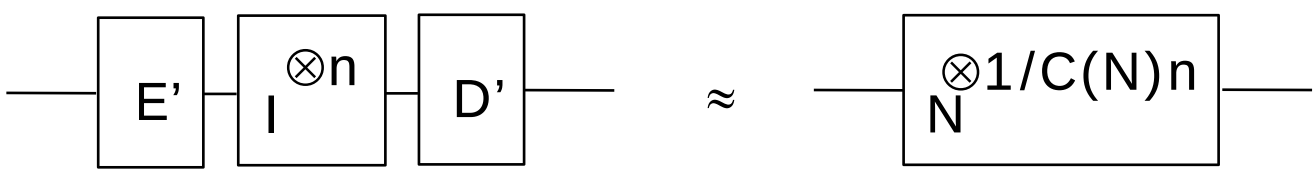
Simulate noiseless channel using noisy channel at the best rate

Capacity C(N) = # qubits sent per channel use




Quantum Reverse Shannon theorem:

Simulate noisy channel N using noisless channel at the rate 1/C(N)




Why?? If true, any channel N can simulate any other channel M

at optimal rate – C(N)/C(M) (N simulates I which simulates M)
so any channel N is characterized by C(N) !

## Quantum reverse Shannon theorem:

- Bennett, Devetak, Harrow, Shor, Winter (0912.5537)
- Berta, Christandl, Renner (0912.3805 – alternative proof)

Proved for tensor-product inputs when entanglement is free but different inputs consume different amount of entanglement so a superposition of inputs is decohered.

Idea: embezzle away the left-over entanglement to keep the coherence of a superposition of inputs!

## Summary:

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