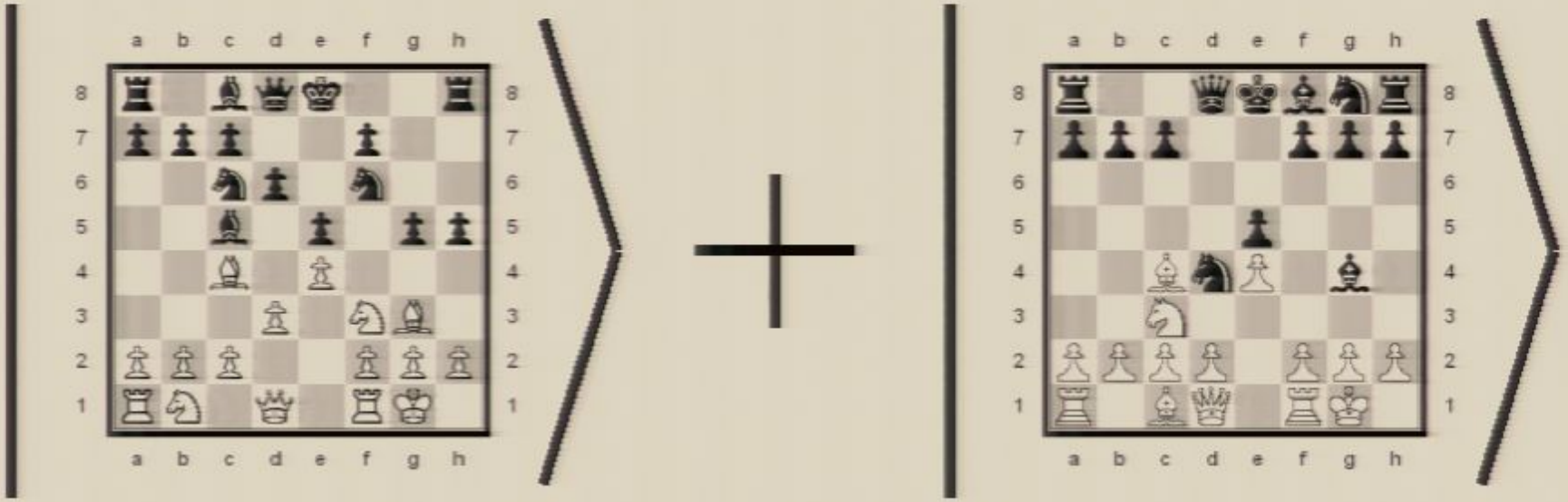
Title: Toward a general theory of quantum games

Date: Jun 04, 2007 03:00 PM

URL: http://pirsa.org/07060024

Abstract:

Semidefinite Representations of Quantum Strategies



Gus Gutoski and John Watrous
IQC, University of Waterloo

quant-ph/0611234

June 4, 2007 at CQISC (Waterloo)

What this talk is about

- **The Goal:**
  To develop formalism for quantum strategies suitable for use in ***any*** interactive quantum protocol. i.e.
  - multiple communicating entities, multiple rounds of communication
  - competitive and/or co-operative
  - e.g. cryptography, communication complexity, computational complexity, distributed computation
- **What We Do:**
  - propose a formalism
  - use it for coin-flipping, min-max theorem, algorithms and complexity.

Quantum Formalism

d-level physical system.

Complex Euclidean space $\mathcal{X} = \mathbb{C}^d$.

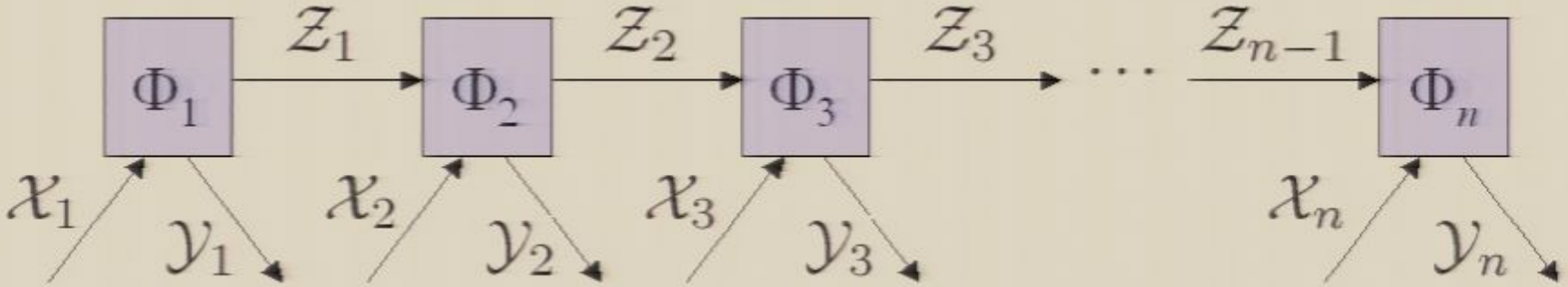
Quantum state.

"Density" operator $\rho \in \mathrm{L}(\mathcal{X})$;
$\rho \geq 0, \mathrm{Tr}(\rho) = 1$.

Quantum operation.

"Super"-operator $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$;
completely positive, trace-preserving.

Quantum Strategy



$$\Phi_1 : \mathrm{L}(\mathcal{X}_1) \to \mathrm{L}(\mathcal{Y}_1 \otimes \mathcal{Z}_1),$$

$$\Phi_i : \mathrm{L}(\mathcal{X}_i \otimes \mathcal{Z}_{i-1}) \to \mathrm{L}(\mathcal{Y}_i \otimes \mathcal{Z}_i),$$

$$\Phi_n : \mathrm{L}(\mathcal{X}_n \otimes \mathcal{Z}_{n-1}) \to \mathrm{L}(\mathcal{Y}_n)$$

$\mathcal{X}_1, \ldots, \mathcal{X}_n$ are *input spaces*
$\mathcal{Y}_1, \ldots, \mathcal{Y}_n$ are *output spaces*
$\mathcal{Z}_1, \ldots, \mathcal{Z}_n$ are *memory spaces*

Quantum Measurement

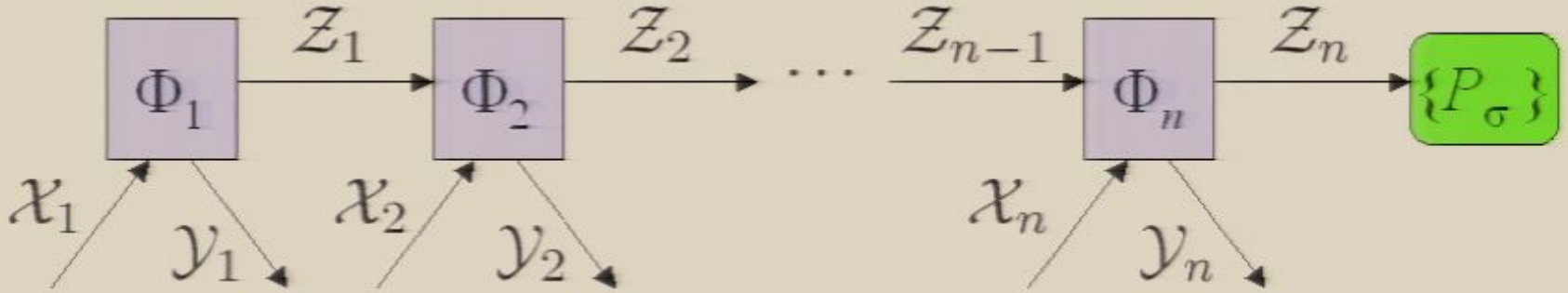
"POVM" operators $\{P_\sigma : \sigma \in \Sigma\} \subset \mathrm{L}(\mathcal{X})$;
Σ is a finite set of *outcomes*,
each $P_\sigma \geq 0$, and

$$\sum_{\sigma \in \Sigma} P_\sigma = I_{\mathcal{X}}.$$

For any state $\rho \in \mathrm{L}(\mathcal{X})$,

$$\Pr[\text{outcome } \sigma] = \langle P_\sigma, \rho \rangle = \mathrm{Tr}(P_\sigma \rho).$$

Measuring Strategy

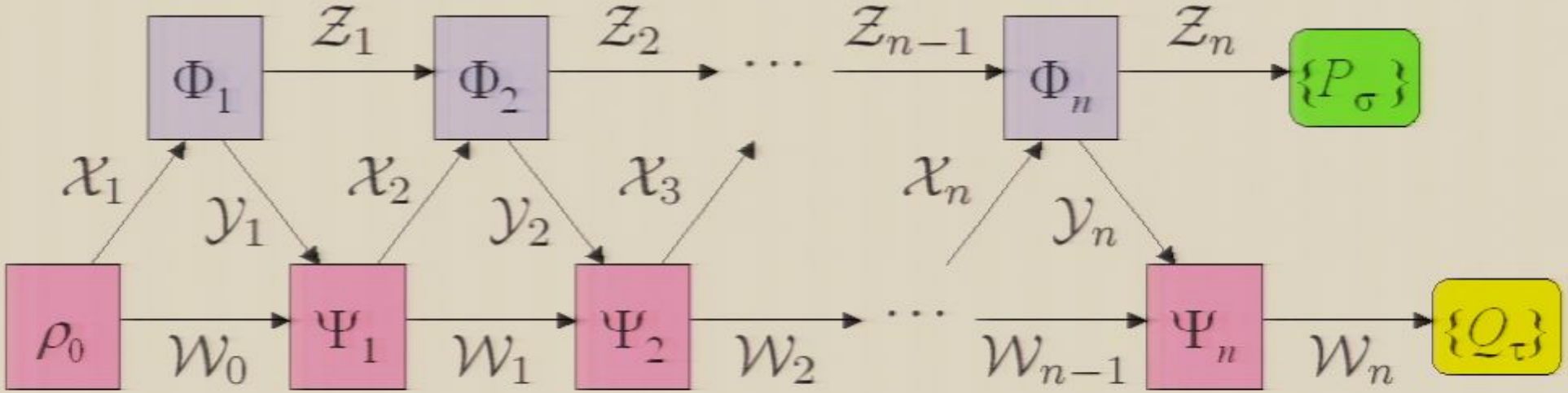


n operations $\Phi_1, \ldots, \Phi_n$ and

one measurement $\{P_\sigma : \sigma \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_n)$.

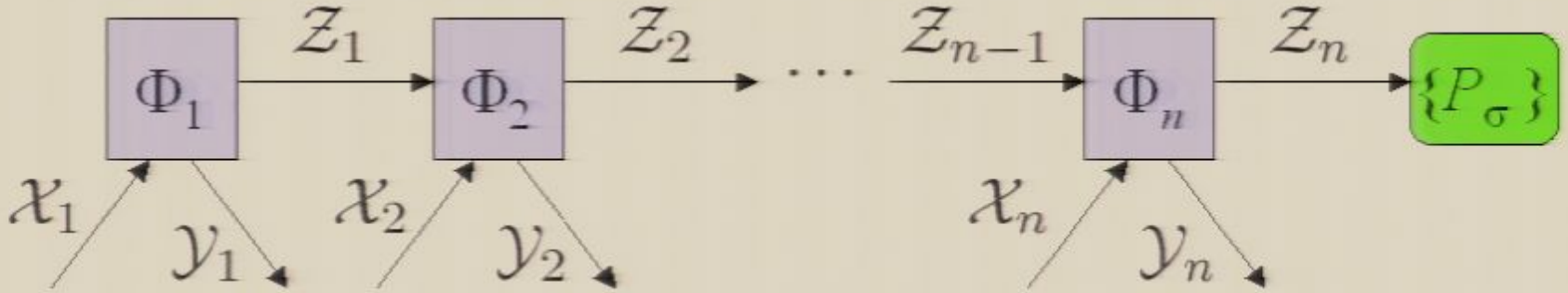
(Multiple intermediate mesurements can be simulated by one measurement at the end.)

Two Interacting Strategies



$A = (\Phi_1, \ldots, \Phi_n, \{P_\sigma\})$ is a *strategy*;
$B = (\rho_0, \Psi_1, \ldots, \Psi_n, \{Q_\tau\})$ is a strategy that is *compatible* with A.

Measuring Strategy

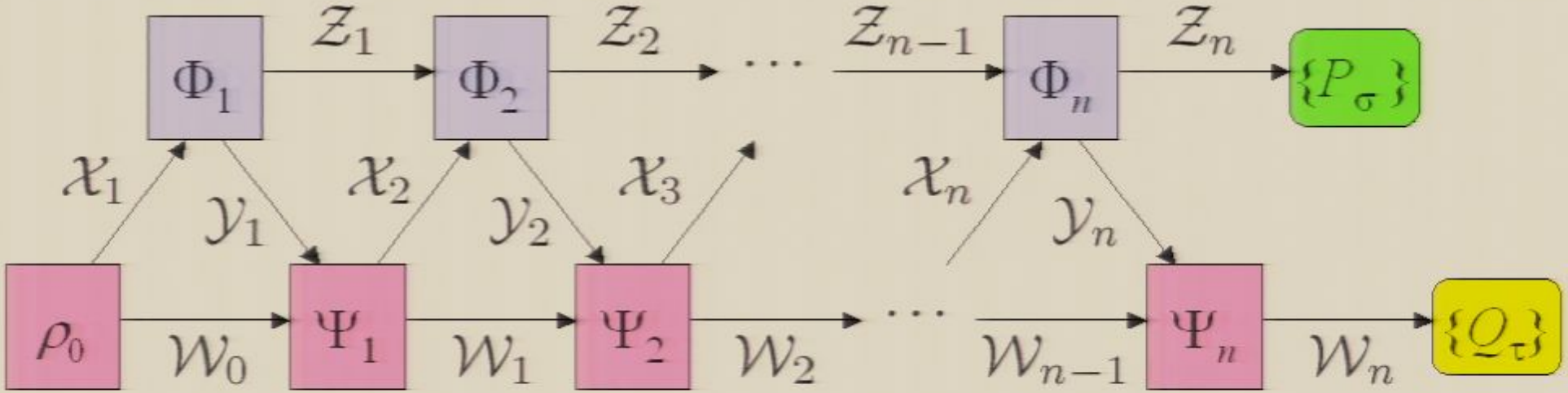


n operations $\Phi_1, \ldots, \Phi_n$ and

one measurement $\{P_\sigma : \sigma \in \Sigma\} \subset \mathrm{L}(\mathcal{Z}_n)$.

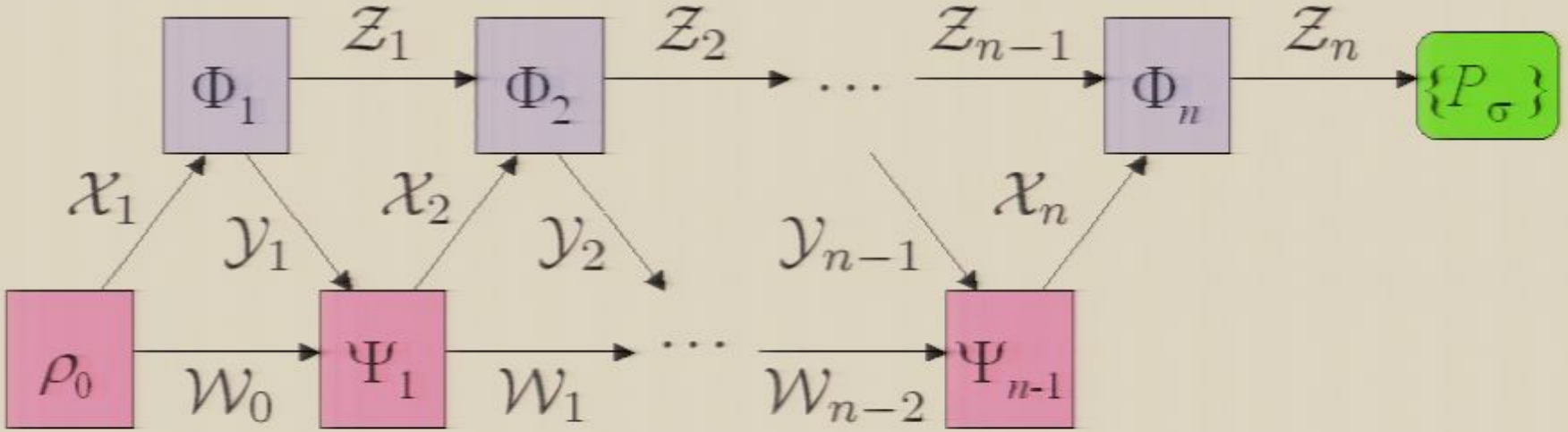
(Multiple intermediate mesurements can be simulated by one measurement at the end.)

Two Interacting Strategies



$A = (\Phi_1, \ldots, \Phi_n, \{P_\sigma\})$ is a *strategy*;
$B = (\rho_0, \Psi_1, \ldots, \Psi_n, \{Q_\tau\})$ is a strategy that is *compatible* with A.

The Big Question



Given: A strategy A and an outcome $\sigma \in \Sigma$.

Question: How do we compute the maximum probability p with which A can be forced to output σ by some compatible strategy?

A Difficult Computation

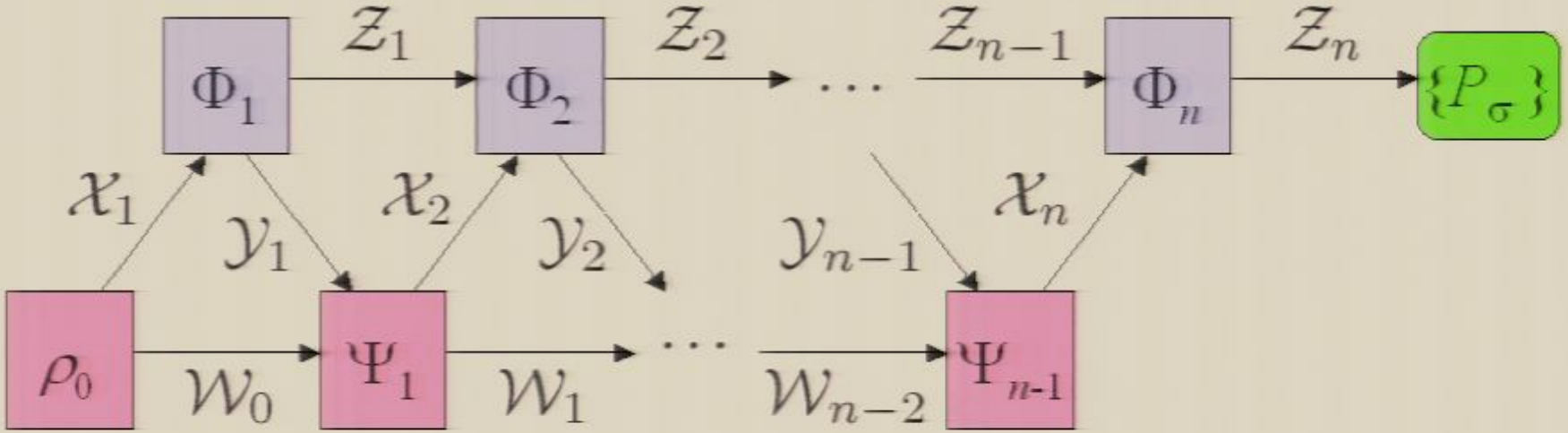
$$p = \max_{B \text{ co-strategy}} \Pr[\text{outcome } \sigma \mid A, B]$$

$$= \max_{B=(\rho_0, \Psi_1, \ldots, \Psi_{n-1})} \langle P_\sigma, \xi_B \rangle$$

where $\xi_B \in \mathrm{L}(\mathcal{Z}_n)$ is the final state:

$$\xi_B = \big(\Phi_n \circ \Psi_{n-1} \circ \cdots \circ \Psi_1 \circ \Phi_1\big)(\rho_0).$$

The Big Question



Given: A strategy A and an outcome $\sigma \in \Sigma$.

Question: How do we compute the maximum probability p with which A can be forced to output σ by some compatible strategy?

A Difficult Computation

$$p = \max_{B \text{ co-strategy}} \Pr[\text{outcome } \sigma \mid A, B]$$

$$= \max_{B=(\rho_0, \Psi_1, \ldots, \Psi_{n-1})} \langle P_\sigma, \xi_B \rangle$$

where $\xi_B \in \mathrm{L}(\mathcal{Z}_n)$ is the final state:

$$\xi_B = \big(\Phi_n \circ \Psi_{n-1} \circ \cdots \circ \Psi_1 \circ \Phi_1\big)(\rho_0).$$

A Difficult Computation

$$p = \max_{B \text{ co-strategy}} \Pr[\text{outcome } \sigma \mid A, B]$$

$$= \max_{B=(\rho_0, \Psi_1, \ldots, \Psi_{n-1})} \langle P_\sigma, \xi_B \rangle$$

where $\xi_B \in \mathrm{L}(\mathcal{Z}_n)$ is the final state:

$$\xi_B = \big(\Phi_n \circ \Psi_{n-1} \circ \cdots \circ \Psi_1 \circ \Phi_1\big)(\rho_0).$$

Multi-linear dependence on Φ_i, Ψ_i, ρ_0.

A Difficult Computation

$$p = \max_{B \text{ co-strategy}} \Pr[\text{outcome } \sigma \mid A, B]$$

$$= \max_{B=(\rho_0, \Psi_1, \ldots, \Psi_{n-1})} \langle P_\sigma, \xi_B \rangle$$

where $\xi_B \in \mathrm{L}(\mathcal{Z}_n)$ is the final state:

$$\xi_B = \big(\Phi_n \circ \Psi_{n-1} \circ \cdots \circ \Psi_1 \circ \Phi_1\big)(\rho_0).$$

Need a better representation for strategies!

Join the Choi-Jamiolkowski Cult!

Choi

Let $\Phi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$.
Define $J(\Phi) \in \mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$ by

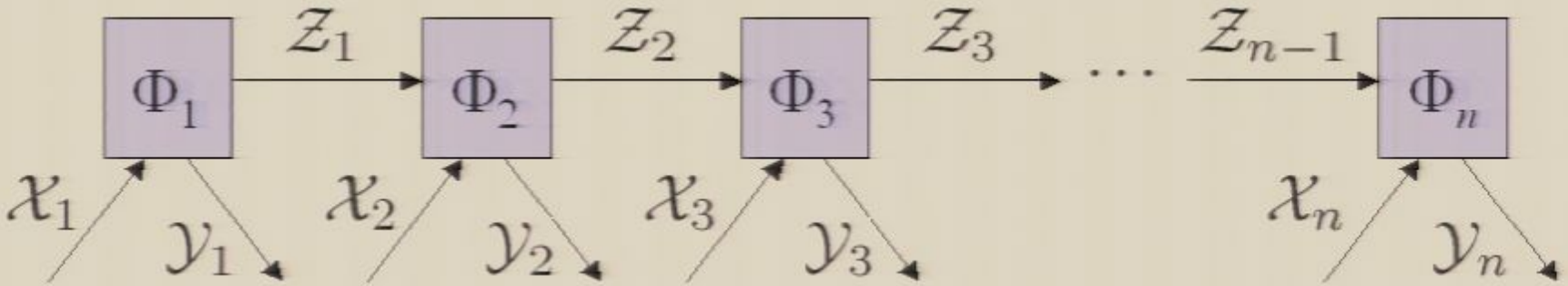
$$J(\Phi) = \sum_{i,j=1}^{\dim(\mathcal{X})} \Phi\big(|i\rangle \langle j| \big) \otimes |i\rangle \langle j| .$$

Jamiolkowski

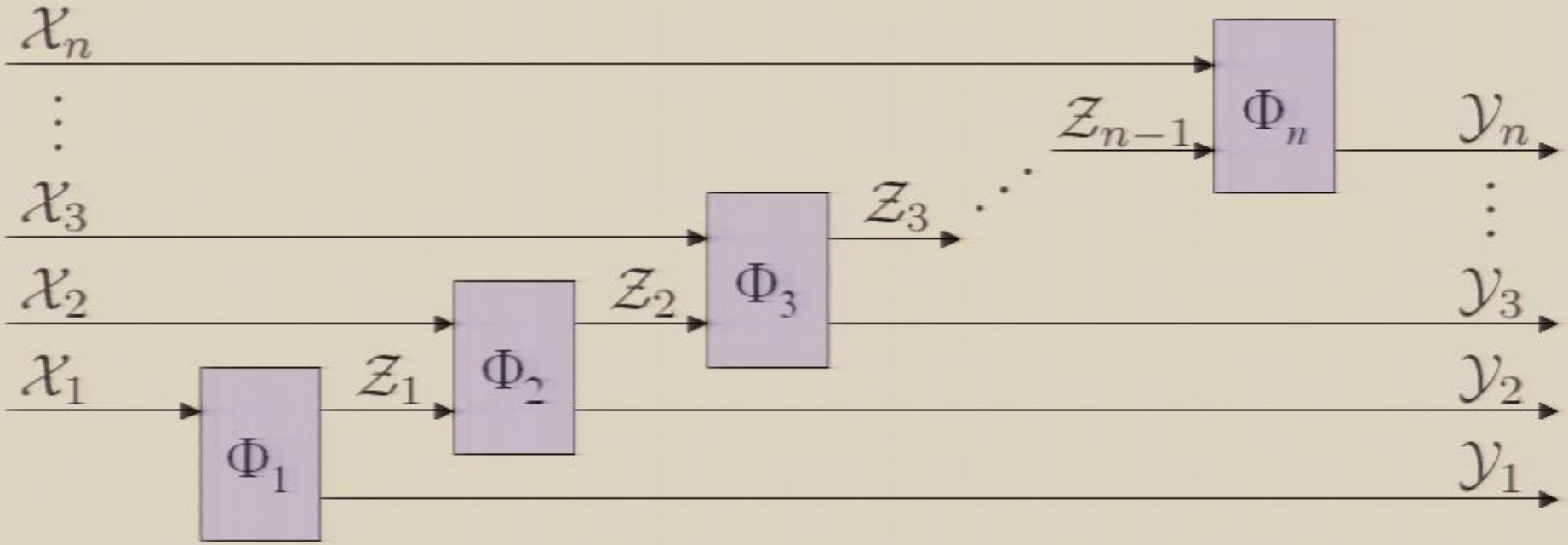
J is an isomorphism.
Φ is completely positive $\Leftrightarrow J(\Phi) \geq 0$.
Φ is trace-preserving $\Leftrightarrow \mathrm{Tr}_{\mathcal{Y}}(J(\Phi)) = I_{\mathcal{X}}$.

Semidefinite Representation

This...


Φ_1
Φ_2
Φ_3
Φ_n
$\mathcal{Z}_1$
$\mathcal{Z}_2$
$\mathcal{Z}_3$
$\cdots$
$\mathcal{Z}_{n-1}$
$\mathcal{X}_1$
$\mathcal{Y}_1$
$\mathcal{X}_2$
$\mathcal{Y}_2$
$\mathcal{X}_3$
$\mathcal{Y}_3$
$\mathcal{X}_n$
$\mathcal{Y}_n$

...is the same as this:



View it as a big super-operator
$\Xi : \mathrm{L}(X_{1:n}) \to \mathrm{L}(\mathcal{Y}_{1:n})$.
Define the *semidefinite representation* as $Q = J(\Xi)$.
That is, $Q \in \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$.

What Were We Thinking?!

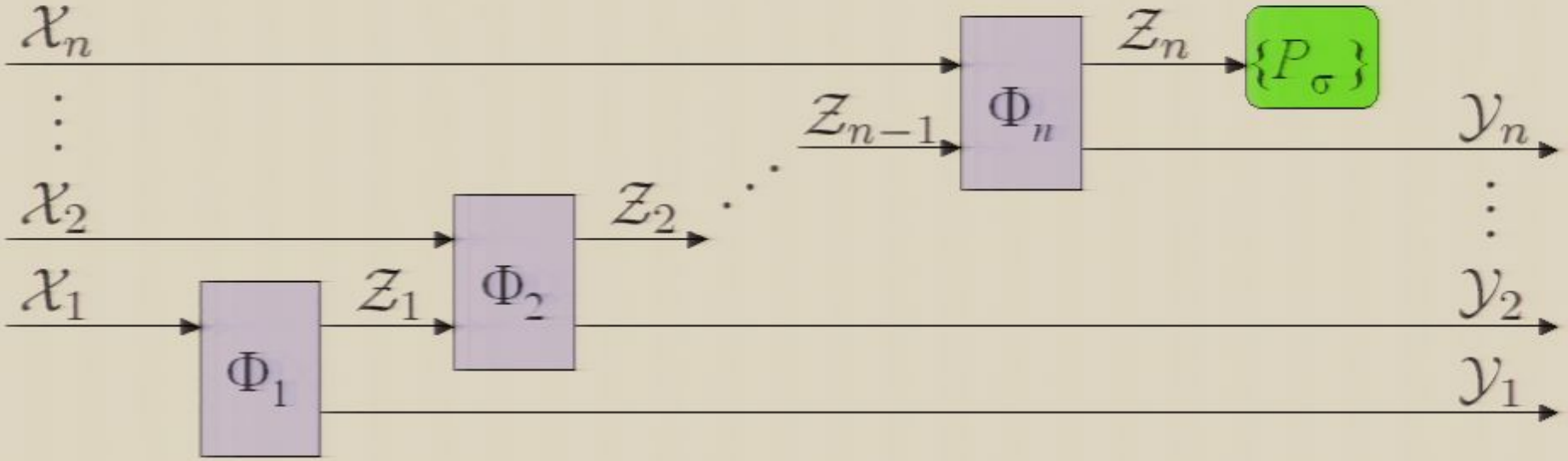
- Given Ξ as a black box physical process, we can ***not*** use Ξ to implement the interaction (unless $n = 1$).
- Physically, Ξ is useless. But mathematically, it is very nice.
- We prove three nice properties of the semidefinite representation.

What Were We Thinking?!

- Given Ξ as a black box physical process, we can ***not*** use Ξ to implement the interaction (unless $n = 1$).
- Physically, Ξ is useless. But mathematically, it is very nice.
- We prove three nice properties of the semidefinite representation.

If there's a Measurement

Let $\{P_\sigma : \sigma \in \Sigma\}$ be a measurement.



View it as a big super-operator

$\Delta : \mathrm{L}(X_{1:n}) \to \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{Z}_n)$.

Measuring Strategies

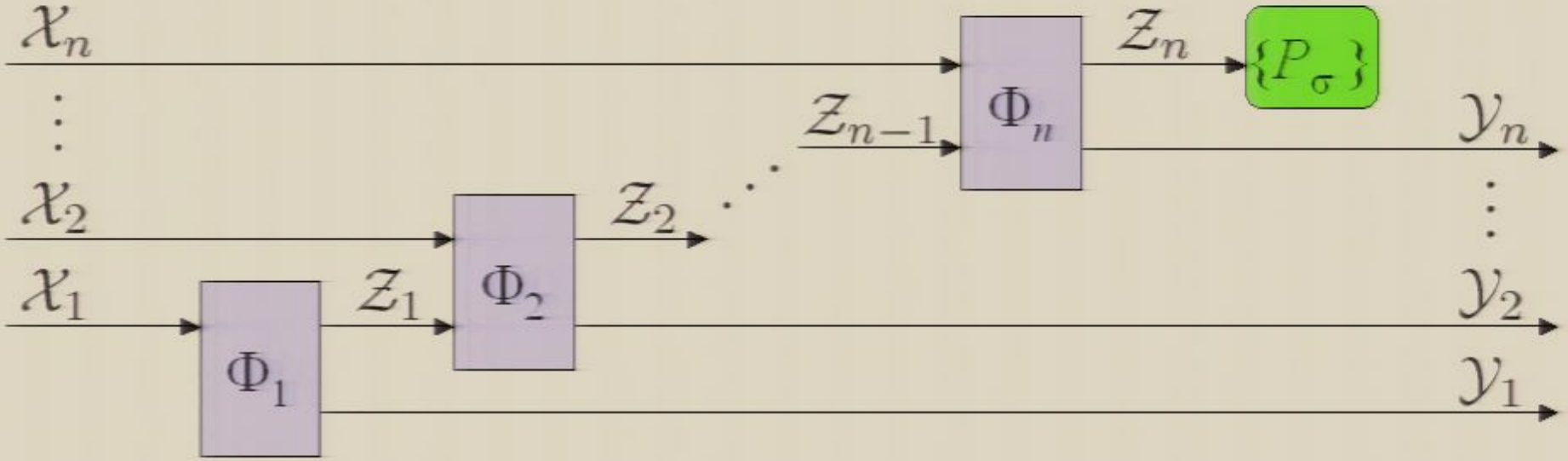
For each $\sigma \in \Sigma$, write

$$\begin{aligned} \Xi_\sigma &: \mathrm{L}(\mathcal{X}_{1:n}) \to \mathrm{L}(\mathcal{Y}_{1:n}) \\ &: X \mapsto \mathrm{Tr}_{\mathcal{Z}_n}((P_\sigma \otimes I_{\mathcal{Y}_{1:n}})\Delta(X)), \\ Q_\sigma &= J(\Xi_\sigma). \end{aligned}$$

The *semidefinite representation* is $\{Q_\sigma : \sigma \in \Sigma\}$.
That is, $\{Q_\sigma\} \subset \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$.

If there's a Measurement

Let $\{P_\sigma : \sigma \in \Sigma\}$ be a measurement.



View it as a big super-operator
$\Delta : \mathrm{L}(X_{1:n}) \to \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{Z}_n)$.

Measuring Strategies

For each $\sigma \in \Sigma$, write

$$\begin{aligned} \Xi_\sigma &: \mathrm{L}(\mathcal{X}_{1:n}) \to \mathrm{L}(\mathcal{Y}_{1:n}) \\ &: X \mapsto \mathrm{Tr}_{\mathcal{Z}_n}((P_\sigma \otimes I_{\mathcal{Y}_{1:n}})\Delta(X)), \\ Q_\sigma &= J(\Xi_\sigma). \end{aligned}$$

The *semidefinite representation* is $\{Q_\sigma : \sigma \in \Sigma\}$.
That is, $\{Q_\sigma\} \subset \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$.

Properties of Strategies

If $\{Q_\sigma : \sigma \in \Sigma\}$ is a measuring strategy then

$$\sum_{\sigma \in \Sigma} Q_\sigma$$

always represents some (non-measuring) strategy.
$\Longrightarrow$ similar in flavour to a POVM measurement.

Without further adieu, three nice properties...

#1: Probabilities of Outcomes

Theorem 1. Let $\{Q_\sigma\}$ and $\{R_\tau\}$ be compatible measuring strategies. Then

$$\Pr[\text{outcome } (\sigma, \tau)] = \mathrm{Tr}\left(Q_\sigma R_\tau^{\mathsf{T}}\right).$$

#2: Linear Characterization

Theorem 2. Let $Q \in \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$. Then Q is a semidefinite representation if and only if:

1. $Q \geq 0$ (completely positive)
2. $\mathrm{Tr}_{\mathcal{Y}_{1:n}}(Q) = I_{\mathcal{X}_{1:n}}$ (trace preserving)
3. For each $j = 2, \ldots, n$ we have

$$\mathrm{Tr}_{\mathcal{Y}_{j:n}}(Q) = Q_{j-1} \otimes I_{\mathcal{X}_{j:n}}$$

for some semidefinite representation Q_{j-1}.

#1: Probabilities of Outcomes

Theorem 1. Let $\{Q_\sigma\}$ and $\{R_\tau\}$ be compatible measuring strategies. Then

$$\Pr[\text{outcome } (\sigma, \tau)] = \mathrm{Tr}\left(Q_\sigma R_\tau^{\mathsf{T}}\right).$$

#2: Linear Characterization

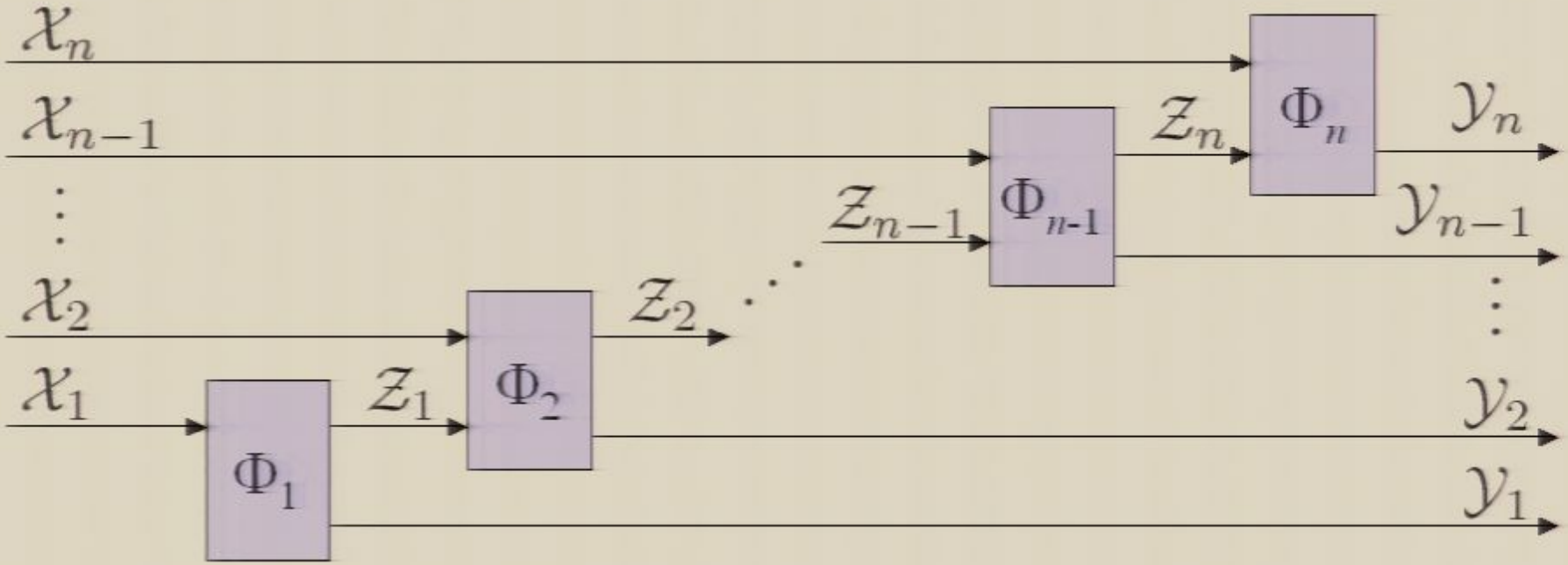
Theorem 2. Let $Q \in \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$. Then Q is a semidefinite representation if and only if:

1. $Q \geq 0$ (completely positive)
2. $\mathrm{Tr}_{\mathcal{Y}_{1:n}}(Q) = I_{\mathcal{X}_{1:n}}$ (trace preserving)
3. For each $j = 2, \ldots, n$ we have

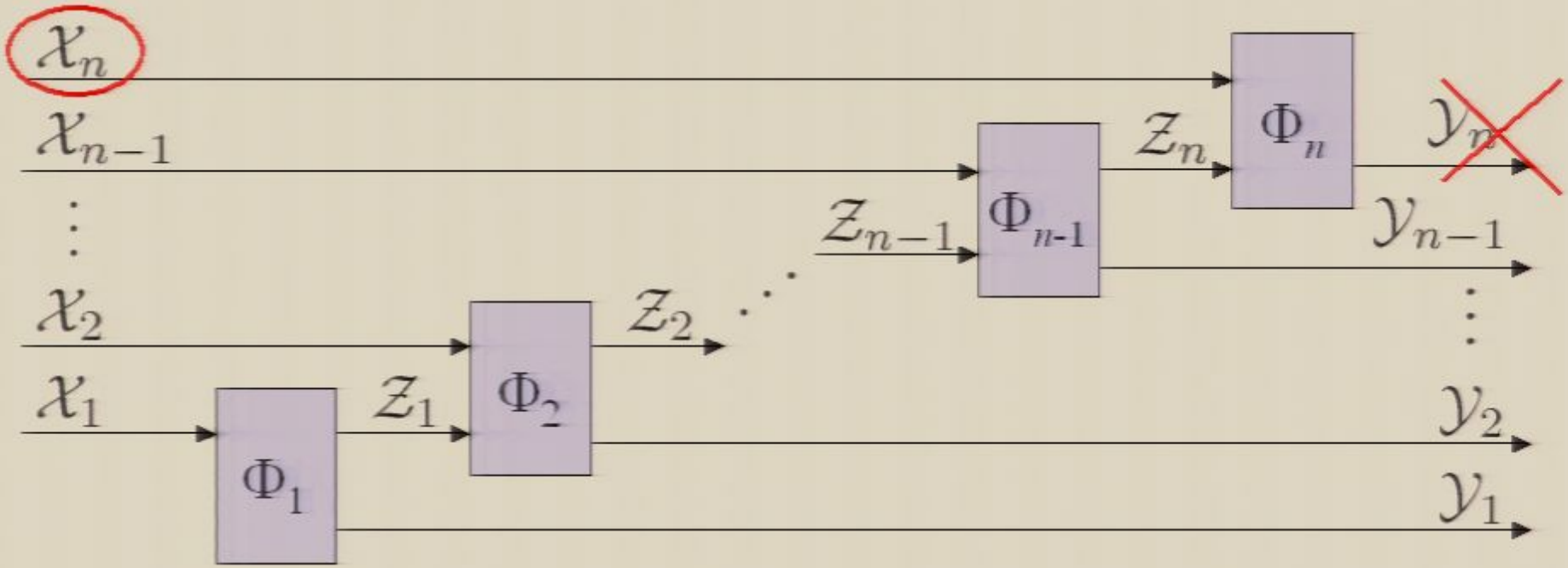
$$\mathrm{Tr}_{\mathcal{Y}_{j:n}}(Q) = Q_{j-1} \otimes I_{\mathcal{X}_{j:n}}$$

for some semidefinite representation Q_{j-1}.

What Theorem 2 Actually Means

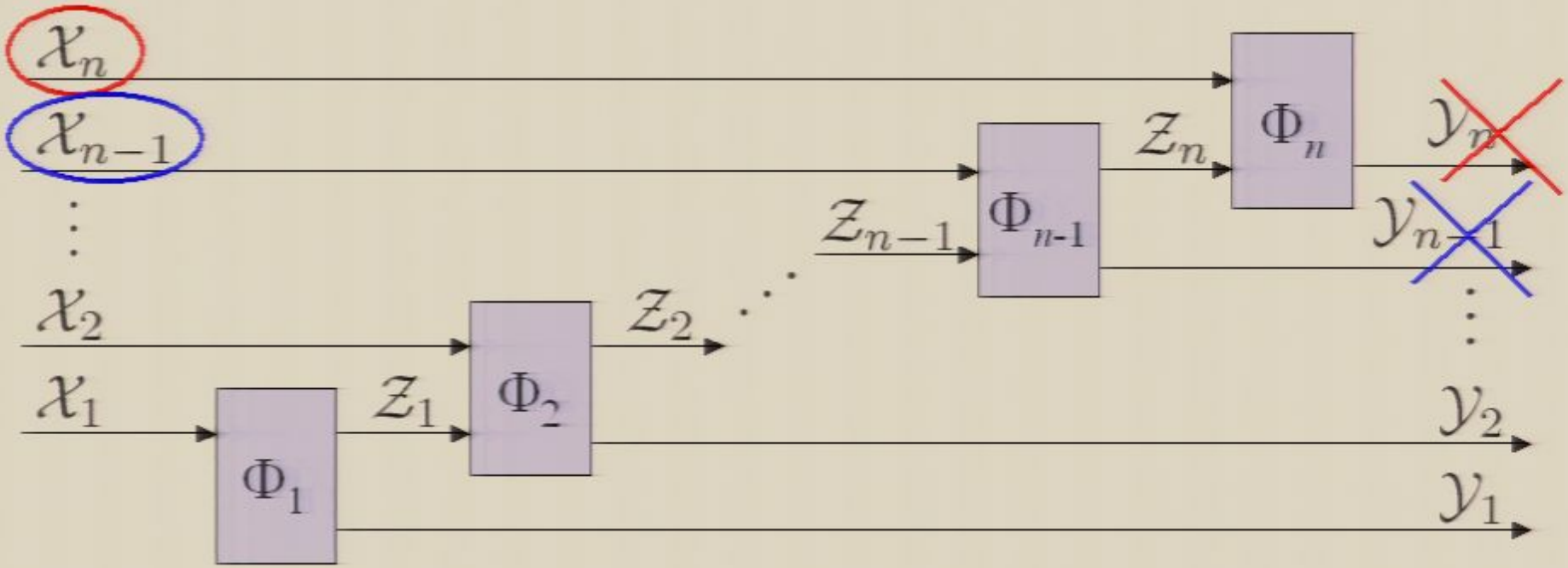


What Theorem 2 Actually Means



Discarding the $\mathcal{Y}_n$ leaves a quantum operation that does not depend on $\mathcal{X}_n$.

What Theorem 2 Actually Means



Discarding the $\mathcal{Y}_n, \mathcal{Y}_{n-1}$ leaves a quantum operation that does not depend on $\mathcal{X}_n, \mathcal{X}_{n-1}$, etc.

#2: Linear Characterization

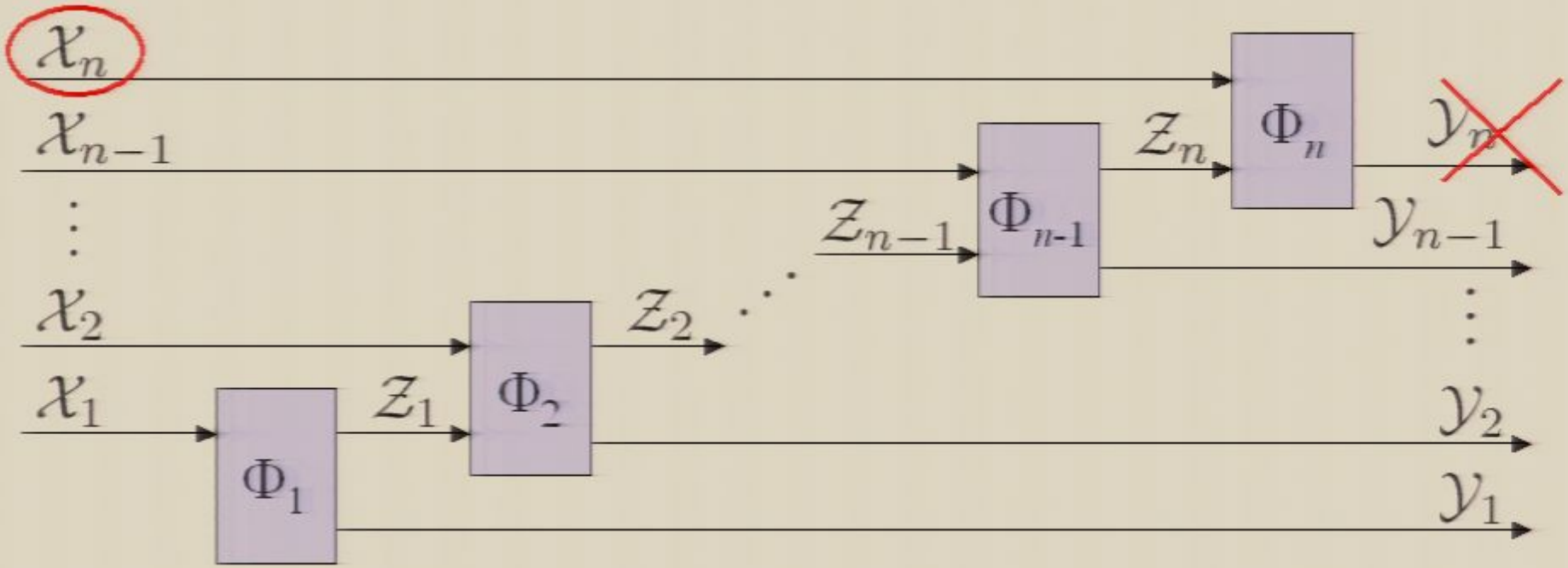
Theorem 2. Let $Q \in \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$. Then Q is a semidefinite representation if and only if:

1. $Q \geq 0$ (completely positive)
2. $\mathrm{Tr}_{\mathcal{Y}_{1:n}}(Q) = I_{\mathcal{X}_{1:n}}$ (trace preserving)
3. For each $j = 2, \ldots, n$ we have

$$\mathrm{Tr}_{\mathcal{Y}_{j:n}}(Q) = Q_{j-1} \otimes I_{\mathcal{X}_{j:n}}$$

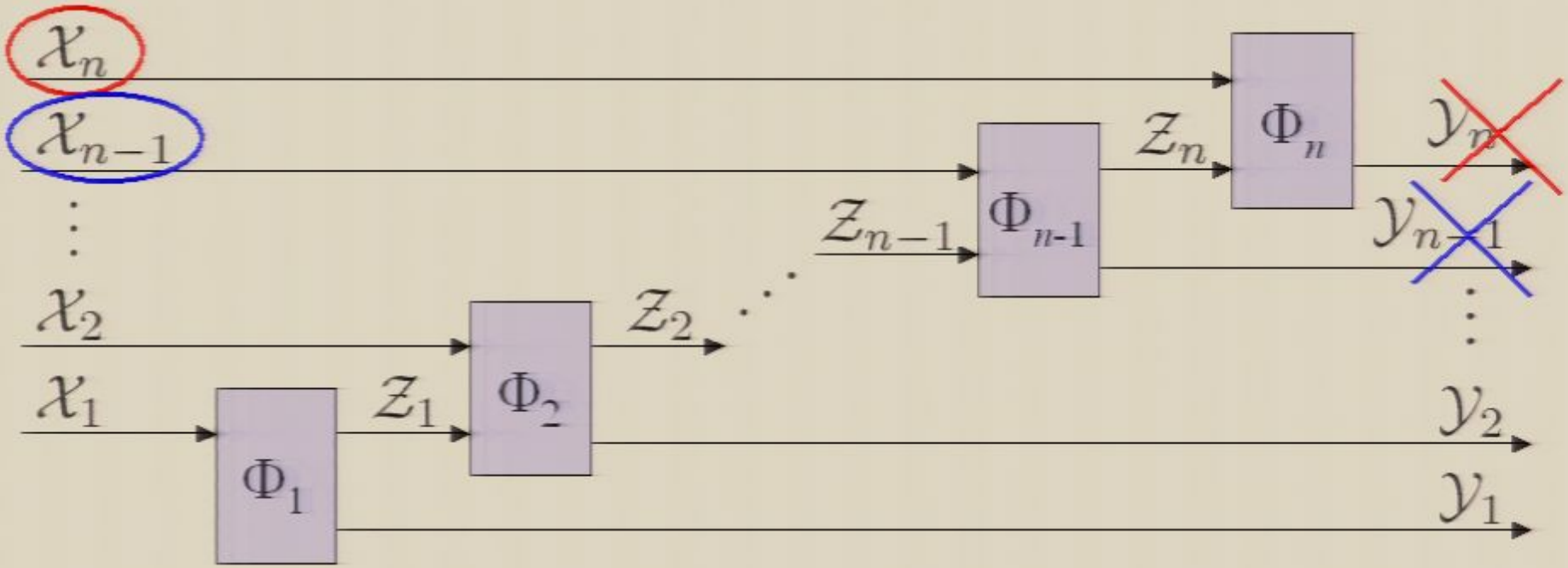
for some semidefinite representation Q_{j-1}.

What Theorem 2 Actually Means



Discarding the $\mathcal{Y}_n$ leaves a quantum operation that does not depend on $\mathcal{X}_n$.

What Theorem 2 Actually Means



Discarding the $\mathcal{Y}_n, \mathcal{Y}_{n-1}$ leaves a quantum operation that does not depend on $\mathcal{X}_n, \mathcal{X}_{n-1}$, etc.

#3: Maximum Output Probability

Let $\mathcal{S}$ be the set of strategies.
Let $\downarrow\mathcal{S} = \{X : 0 \leq X \leq Y, Y \in \mathcal{S}\}$ be the set of *substrategies*.
e.g. any measuring strategy $\{Q_\sigma\} \subset \downarrow\mathcal{S}$.

Theorem 3. Let $\{Q_\sigma\} \subset \downarrow\mathcal{S}$ be any measuring strategy. The maximum probability with which $\{Q_\sigma\}$ can be made to output σ is the ***minimum*** $p \in [0, 1]$ for which $Q_\sigma \in p\downarrow\mathcal{S}$.

#2: Linear Characterization

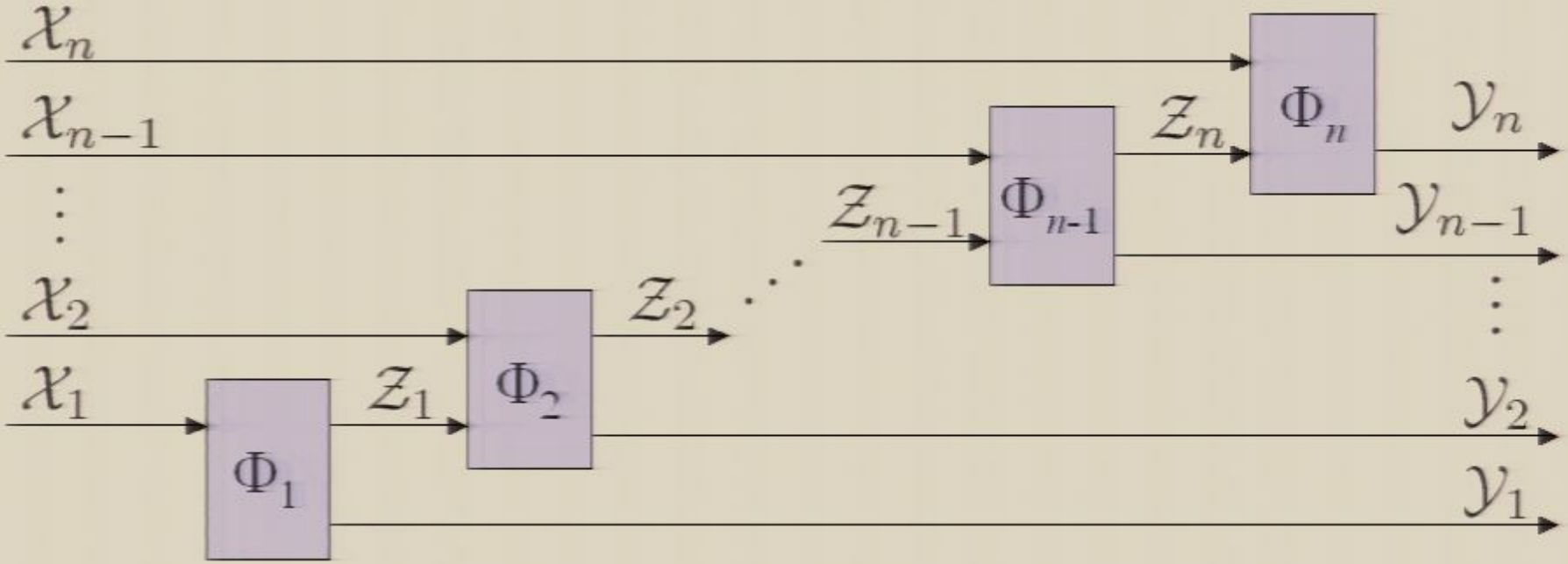
Theorem 2. Let $Q \in \mathrm{L}(\mathcal{Y}_{1:n} \otimes \mathcal{X}_{1:n})$. Then Q is a semidefinite representation if and only if:

1. $Q \geq 0$ (completely positive)
2. $\mathrm{Tr}_{\mathcal{Y}_{1:n}}(Q) = I_{\mathcal{X}_{1:n}}$ (trace preserving)
3. For each $j = 2, \ldots, n$ we have

$$\mathrm{Tr}_{\mathcal{Y}_{j:n}}(Q) = Q_{j-1} \otimes I_{\mathcal{X}_{j:n}}$$

for some semidefinite representation Q_{j-1}.

What Theorem 2 Actually Means

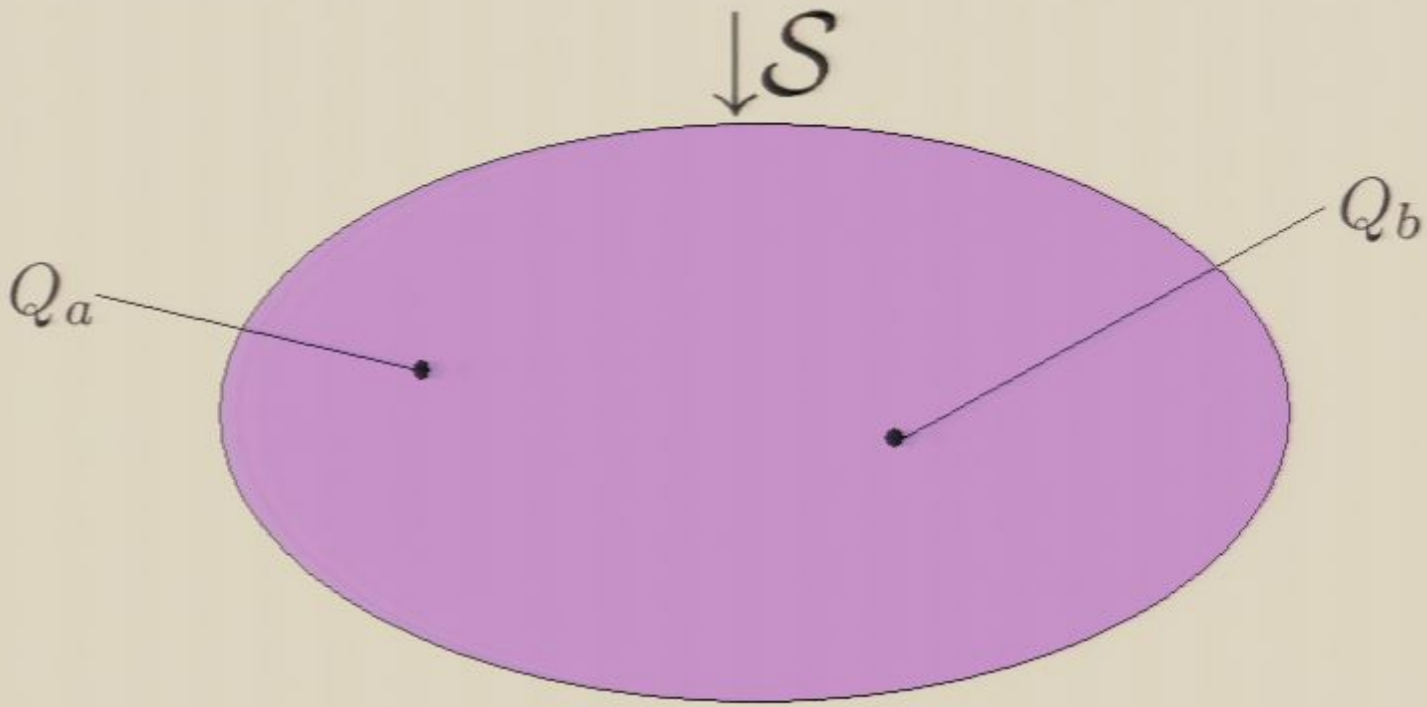


#3: Maximum Output Probability

Let $\mathcal{S}$ be the set of strategies.
Let $\downarrow\mathcal{S} = \{X : 0 \leq X \leq Y, Y \in \mathcal{S}\}$ be the set of *substrategies*.
e.g. any measuring strategy $\{Q_\sigma\} \subset \downarrow\mathcal{S}$.

Theorem 3. Let $\{Q_\sigma\} \subset \downarrow\mathcal{S}$ be any measuring strategy. The maximum probability with which $\{Q_\sigma\}$ can be made to output σ is the ***minimum*** $p \in [0, 1]$ for which $Q_\sigma \in p\downarrow\mathcal{S}$.

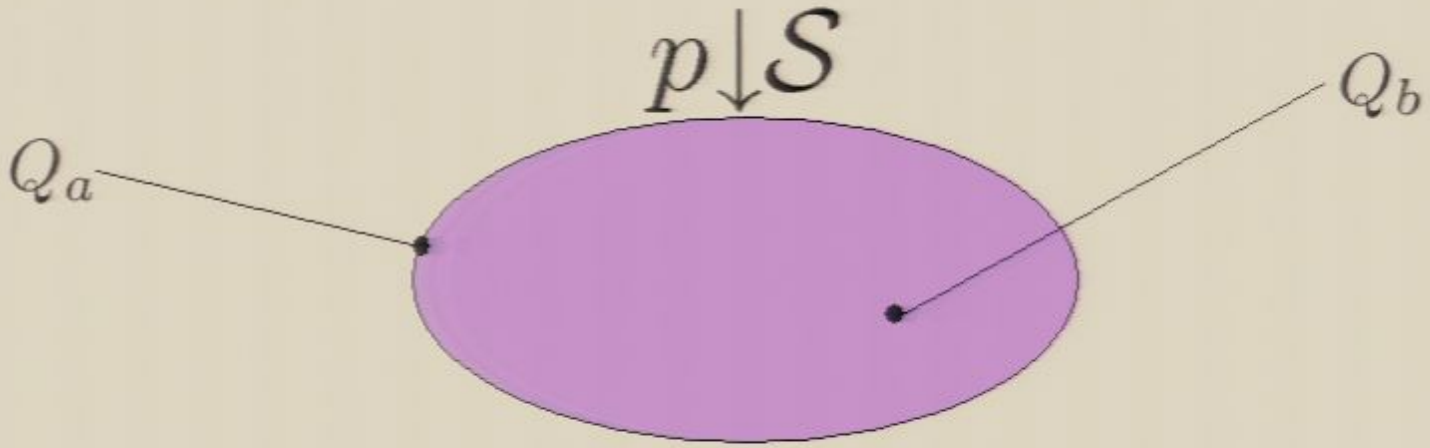
What Theorem 3 Actually Means



$$Q_a, Q_b \in 1 \cdot \downarrow S$$

What Theorem 3 Actually Means

Let $0 < p < 1$.

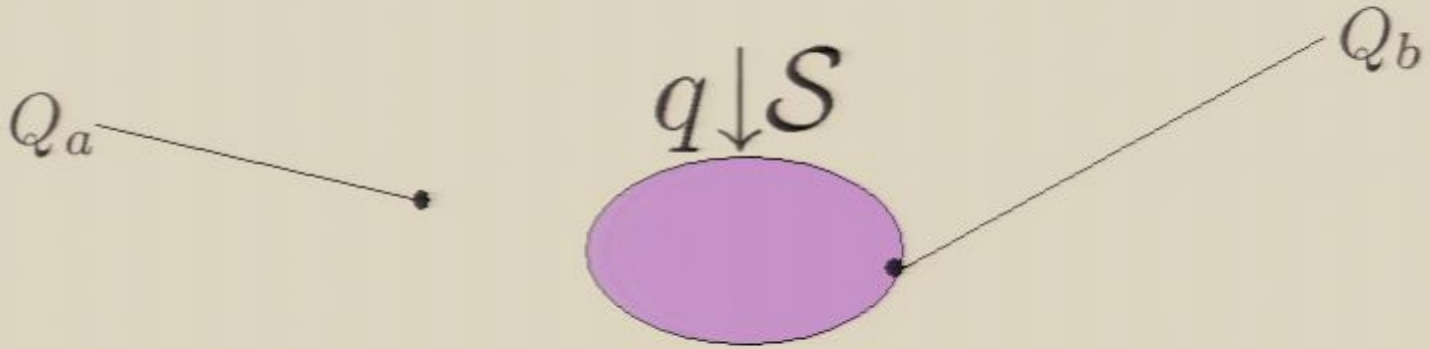


$Q_a \in p{\downarrow}\mathcal{S}$, but $Q_a \notin p'{\downarrow}\mathcal{S}$ for any $p' < p$.

$\Longrightarrow \max \Pr[\text{outcome } a] = p.$

What Theorem 3 Actually Means

Let $0 < q < p$.



$Q_b \in q{\downarrow}\mathcal{S}$, but $Q_b \notin q'{\downarrow}\mathcal{S}$ for any $q' < q$.

$\Longrightarrow \max \Pr[\text{outcome } b] = q < p.$

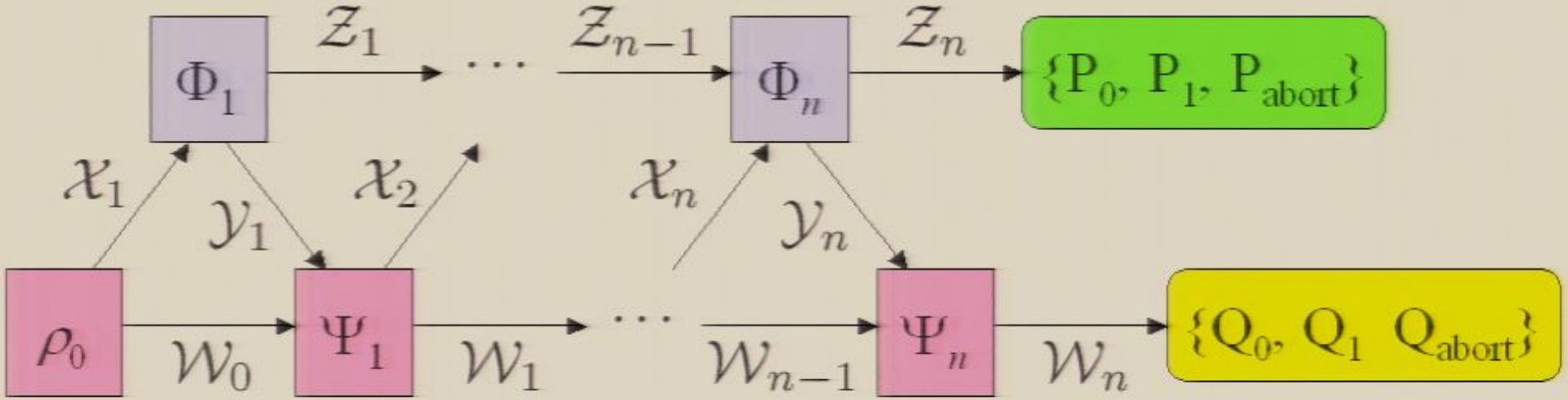
Thm. 3 Measurement Analogy

Let $\{P_\sigma : \sigma \in \Sigma\}$ be a measurement.
Let p be the maximum probability with which $\{P_\sigma\}$ can be made to output σ.

- Clearly, $p = \| P_\sigma \|$.
- Equivalently, $p = \min\{q : P_\sigma \leq qI\}$.

Application 1: Coin-Flipping

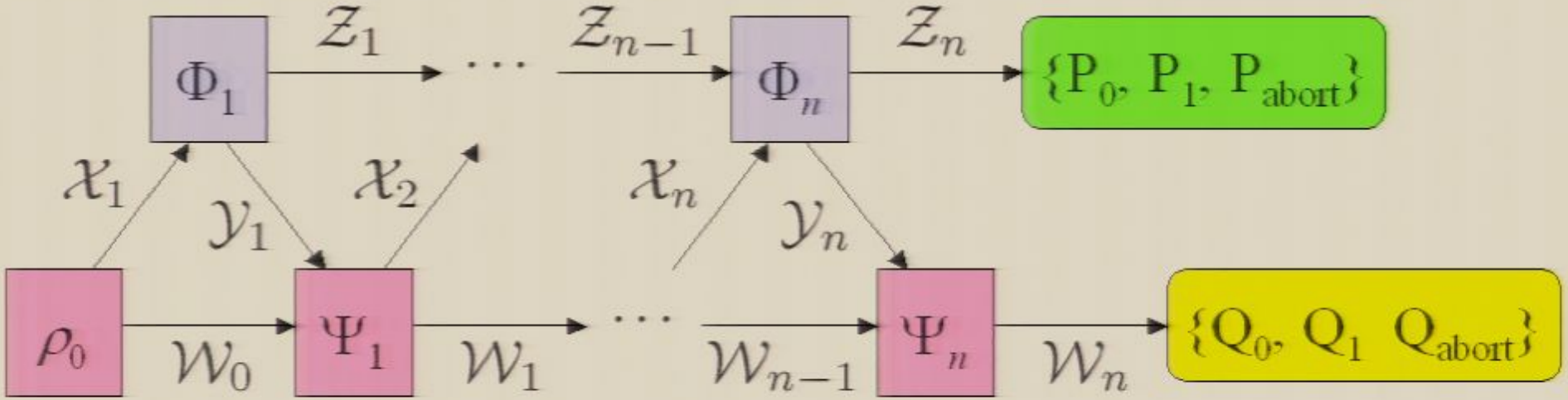
Coin-Flipping Interaction



Alice: $(\rho_0, \Psi_1, \ldots, \Psi_n, \{Q_\tau\})$,
Bob: $(\Phi_1, \ldots, \Phi_n, \{P_\sigma\})$.
(Alice and Bob are compatible.)

Application 1: Coin-Flipping

Coin-Flipping Interaction



Alice: $(\rho_0, \Psi_1, \ldots, \Psi_n, \{Q_\tau\})$,
Bob: $(\Phi_1, \ldots, \Phi_n, \{P_\sigma\})$.
(Alice and Bob are compatible.)

Coin-Flipping – The Rules

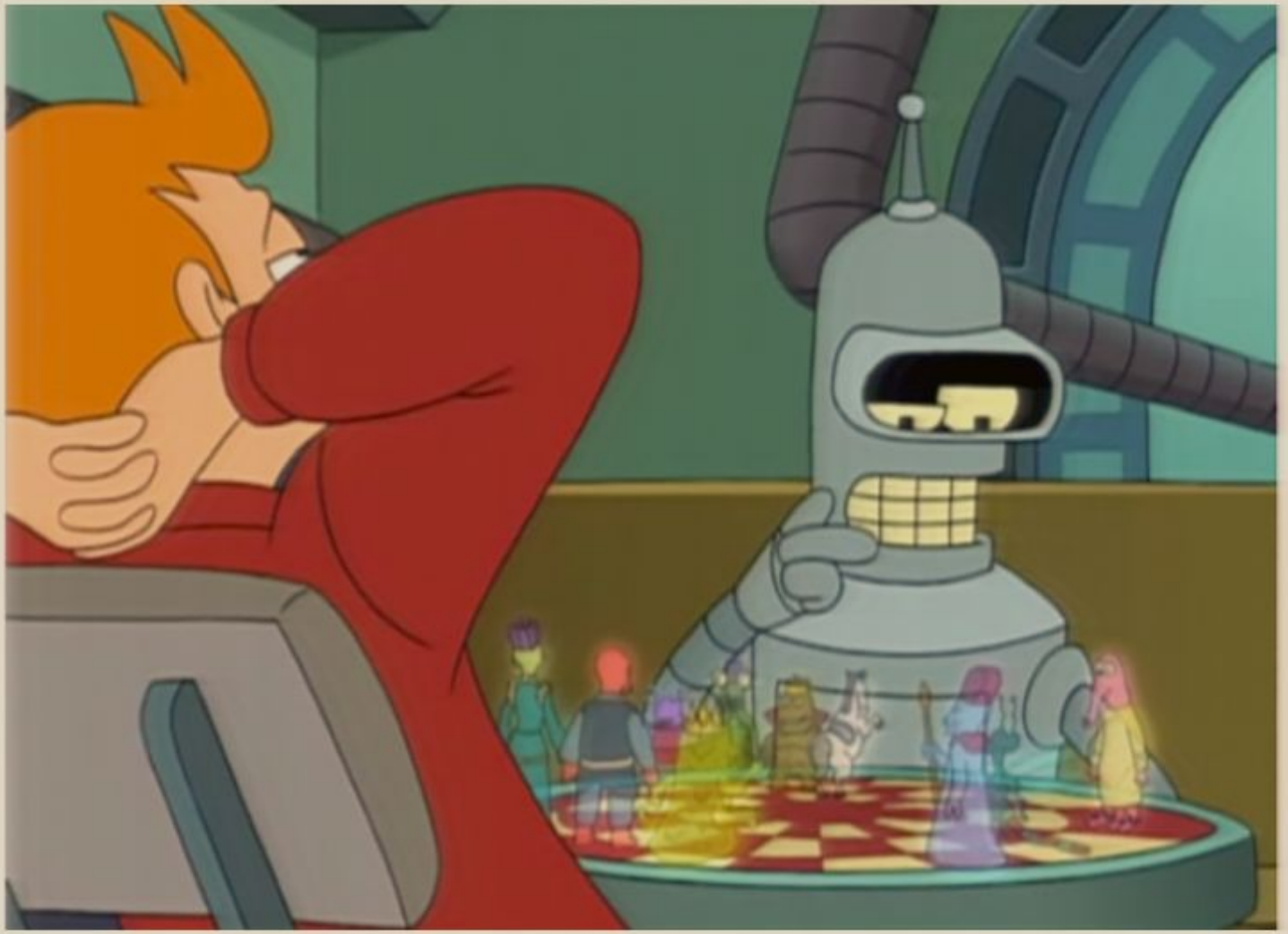
- Alice and Bob want to agree on a random $b \in \{0,1\}$
- They don't trust each other
- They exchange (quantum) messages, then perform a measurement {0,1,abort}
- If Alice and Bob are both honest then we require $Pr[0] = Pr[1] = ½$
- If Alice cheats, with what probability can she convince honest Bob to output $b \in \{0,1\}$?

Kitaev's Bound on One Slide

Known: one cheating party can always force a given outcome on an honest party w/prob at least $\frac{1}{\sqrt{2}}$.

Alternate Proof. Honest Alice $= \{A_0, A_1, A_{\text{abort}}\}$, honest Bob $= \{B_0, B_1, B_{\text{abort}}\}$.
Then $\frac{1}{2} = \text{Tr}(A_0 B_0^\mathsf{T}) = \text{Tr}(A_1 B_1^\mathsf{T})$ (Theorem 1).
Suppose honest Alice can be forced to output $b \in \{0,1\}$ w/prob $p \in [\frac{1}{2}, \frac{1}{\sqrt{2}}]$.
Then $\frac{1}{p} A_b \in \downarrow\mathcal{S}$ (Theorem 3), hence there exists cheating Alice $\{A'_0, A'_1, A'_{\text{abort}}\}$ with $A'_b = \frac{1}{p} A_b$.
Then $\text{Tr}(A'_b B_b^\mathsf{T}) = \frac{1}{p}\text{Tr}(A_b B_b^\mathsf{T}) = \frac{1}{2p} \geq \frac{1}{\sqrt{2}}$. $\square$

Application 2: Quantum Min-Max



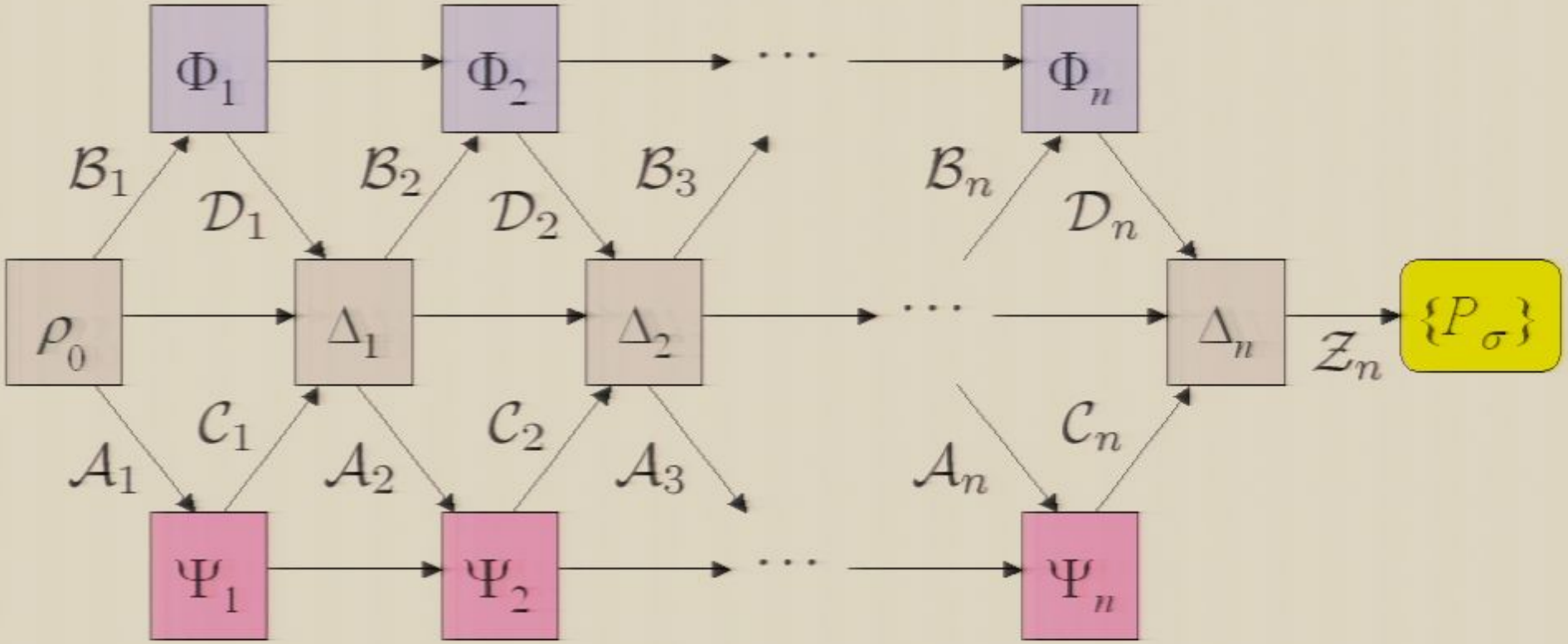
"Horsey to pointy-guy six..."

Several Ways to Model a Game

Classically:

- Games can be formalized in many ways
  - e.g. tree of moves, payoff matrix, etc.
- The formalization that "quantizes" best is the **refereed games model**

Refereed Game Interaction



$$Alice : (\Psi_1, \ldots, \Psi_n),$$

$$Bob : (\Phi_1, \ldots, \Phi_n),$$

$$Referee : (\rho_0, \Delta_1, \ldots, \Delta_n, \{P_\sigma\}).$$

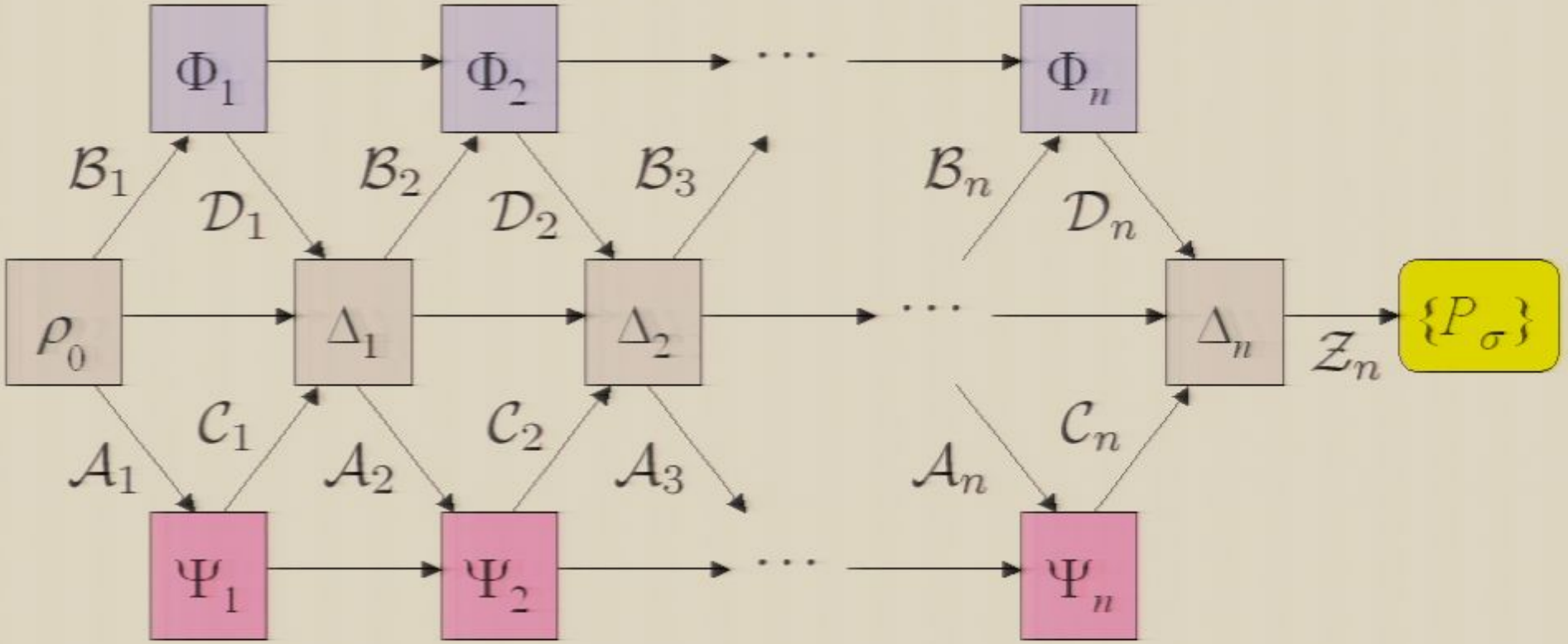
Refereed Game Strategies

Semidefinite representations:

$$\begin{aligned} \textit{Alice} &: A \in \mathrm{L}(\mathcal{C}_{1:n} \otimes \mathcal{A}_{1:n}), \\ \textit{Bob} &: B \in \mathrm{L}(\mathcal{D}_{1:n} \otimes \mathcal{B}_{1:n}), \\ \textit{Referee} &: \{R_{\mathrm{Alice}}, R_{\mathrm{Bob}}\} \\ &\qquad \subset \mathrm{L}((\mathcal{A}_{1:n} \otimes \mathcal{B}_{1:n}) \otimes (\mathcal{C}_{1:n} \otimes \mathcal{D}_{1:n})). \end{aligned}$$

($A \otimes B$ is compatible with $\{R_{\mathrm{Alice}}, R_{\mathrm{Bob}}\}$.)

Refereed Game Interaction



$$Alice : (\Psi_1, \ldots, \Psi_n),$$

$$Bob : (\Phi_1, \ldots, \Phi_n),$$

$$Referee : (\rho_0, \Delta_1, \ldots, \Delta_n, \{P_\sigma\}).$$

Refereed Game Strategies

Semidefinite representations:

$$\begin{aligned} \textit{Alice} &: A \in \mathrm{L}(\mathcal{C}_{1:n} \otimes \mathcal{A}_{1:n}), \\ \textit{Bob} &: B \in \mathrm{L}(\mathcal{D}_{1:n} \otimes \mathcal{B}_{1:n}), \\ \textit{Referee} &: \{R_{\mathrm{Alice}}, R_{\mathrm{Bob}}\} \\ &\qquad \subset \mathrm{L}((\mathcal{A}_{1:n} \otimes \mathcal{B}_{1:n}) \otimes (\mathcal{C}_{1:n} \otimes \mathcal{D}_{1:n})). \end{aligned}$$

($A \otimes B$ is compatible with $\{R_{\mathrm{Alice}}, R_{\mathrm{Bob}}\}$.)

Quantum Min-Max Theorem

$$\Pr[\text{Bob wins} \mid A, B] = \mathrm{Tr}\left(R_{\mathrm{Bob}}(A \otimes B)^{\mathsf{T}}\right)$$

linear in A,B

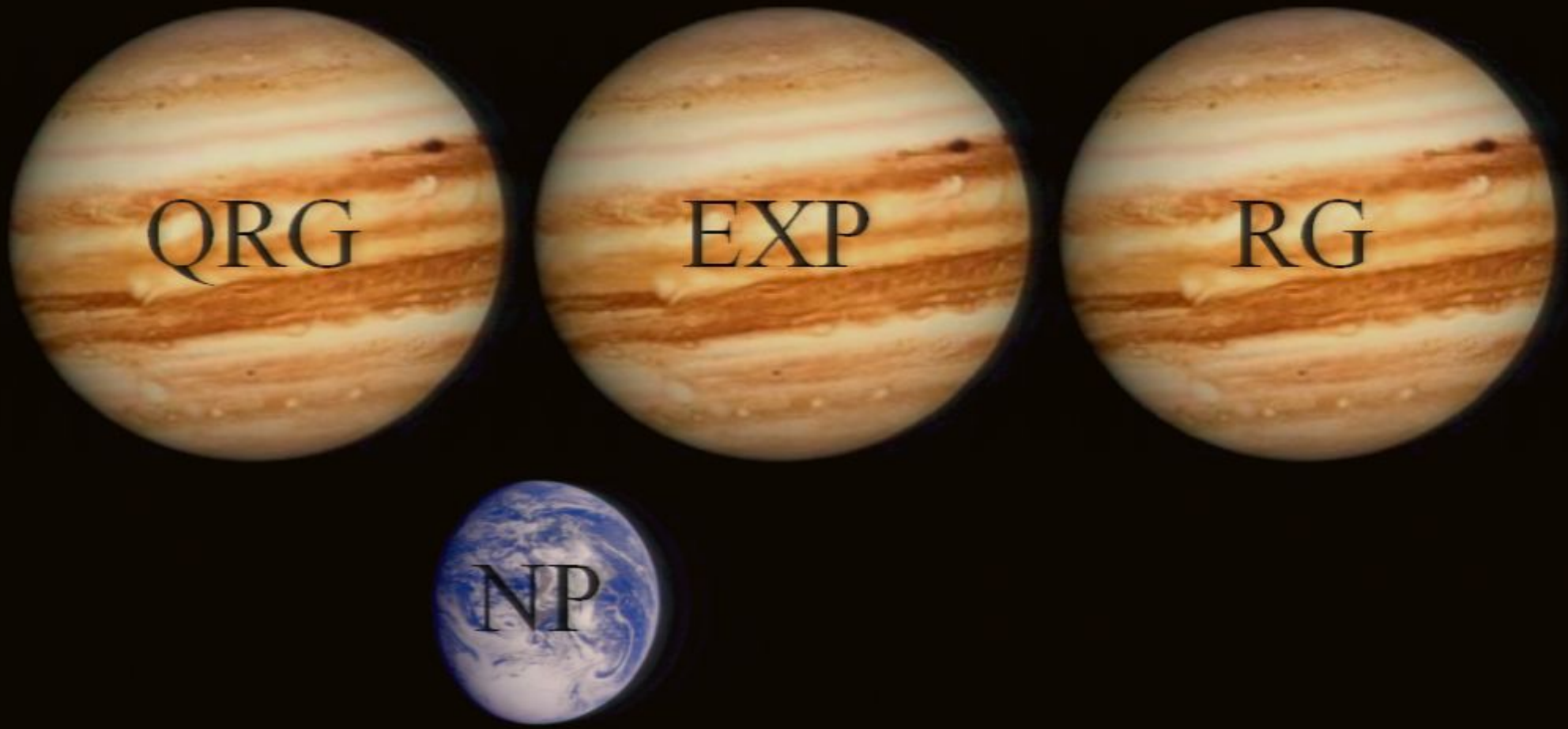
Quantum min-max theorem:

$$\min_A \max_B \Pr[\text{Bob wins} \mid A, B]$$

$$= \max_B \min_A \Pr[\text{Bob wins} \mid A, B]$$

convex sets

Application 3: Algorithms and Complexity



The Refereed Games Problem

Problem. Quantum Refereed Games

Input. a referee's measuring strategy
$\{R_{\text{Alice}}, R_{\text{Bob}}\}$

Output. Bob's maximum success probability.
In other words:

$$\max_{B} \min_{A} \text{Tr}\left(R_{\text{Bob}}(A \otimes B)^{\mathsf{T}}\right)$$

Some Notation

$\{R_{\text{Alice}}, R_{\text{Bob}}\} \subset \downarrow\mathcal{S}(\text{Referee})$
Set of Alice's strategies: $\mathcal{S}(\text{Alice})$
Set of Bob's strategies: $\mathcal{S}(\text{Bob})$
Strategies can be combined:
e.g. Alice's strategy $A \in \mathcal{S}(\text{Alice})$ can be "hard-wired" into the referee to get a new strategy:

$$\{(R|A)_{\text{Alice}}, (R|A)_{\text{Bob}}\} \subset \downarrow\mathcal{S}(\text{Alice} + \text{Referee}).$$

$(R|A)_{\text{Alice}}$ is bilinear in R_{Alice} and A,
$(R|A)_{\text{Bob}}$ is bilinear in R_{Bob} and A.

Semidefinite Optimization

$$\begin{aligned} \text{minimize} \quad & p \\ \text{subject to} \quad & A \in \mathcal{S}(\text{Alice}) \\ & (R|A)_{\text{Bob}} \in p{\downarrow}\mathcal{S}(\text{Alice} + \text{Referee}) \end{aligned}$$

- The constraints of this optimization problem are all linear or semidefinite.
- Can be solved deterministically in time polynomial in dimension of matrices (exponential in the number of qubits).

Complexity Theory

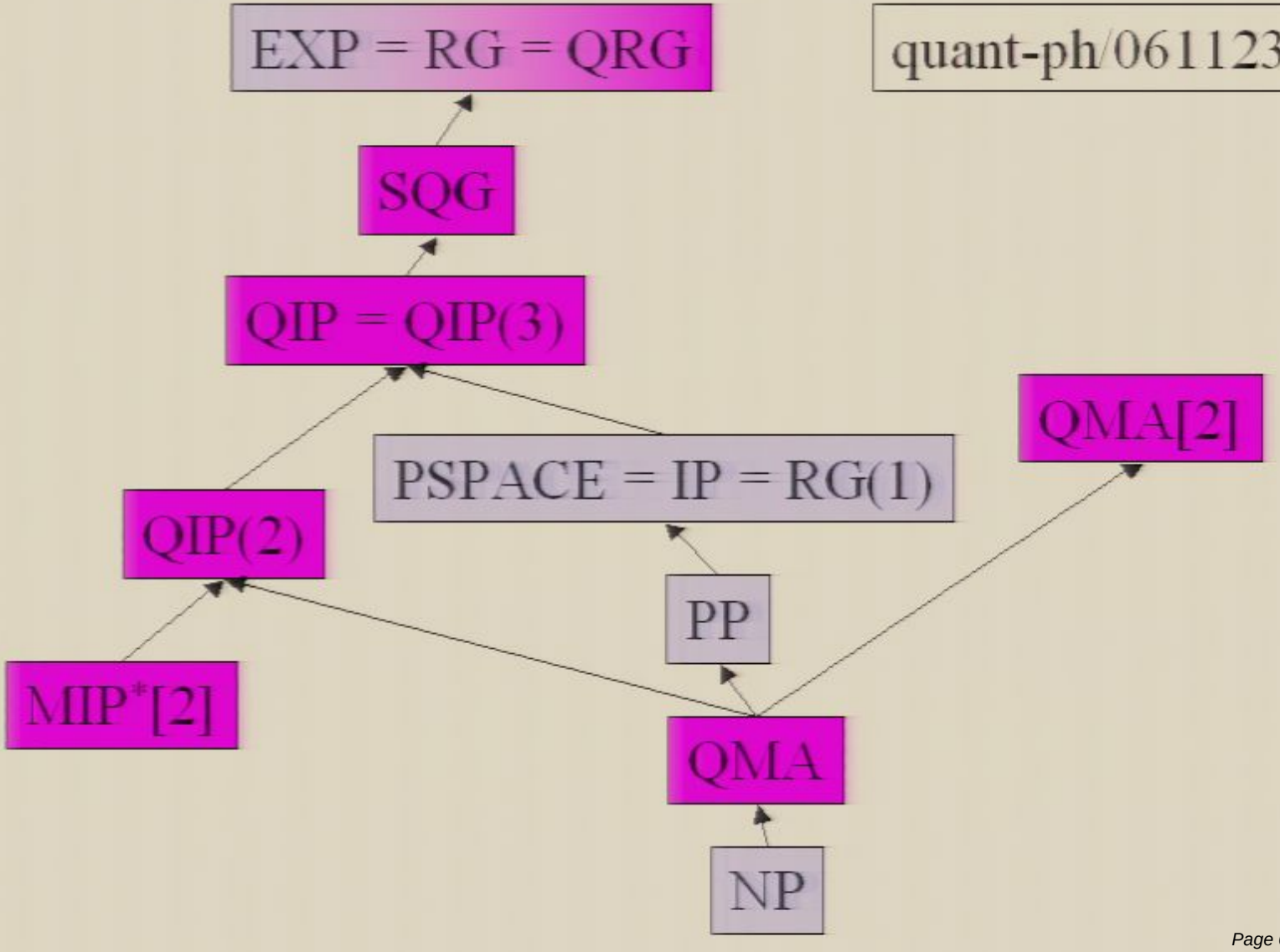
QRG: class of languages that have a quantum refereed game (*i.e.* quantum interactive proof with competing provers).

EXP: class of languages decidable in deterministic exponential time.

$\Longrightarrow$ we showed QRG $\subseteq$ EXP.

[Feige-Kilian 1997] showed EXP $\subseteq$ RG.
$\Longrightarrow$ QRG = RG = EXP.
(RG = EXP was already known [FK97,KM92])

Fin


EXP = RG = QRG
quant-ph/0611234
SQG
QIP = QIP(3)
QMA[2]
PSPACE = IP = RG(1)
QIP(2)
PP
MIP*[2]
QMA
NP