quantum information theory group

PRL **101** 060401 (2008)
PRL **101** 180501 (2008)
PRL **101** 180504 (2008)
PRL **102** 010404 (2009)
EL **83** 30004 (2008)

The quantum comb: theory and applications to quantum networks

Giacomo Mauro D'Ariano

QUIT group, University of Pavia

Institute for Theoretical Physics, University of Innsbruck,
"Seminar/Theory Colloquium", March 19 2009

QUIT Group in Pavia

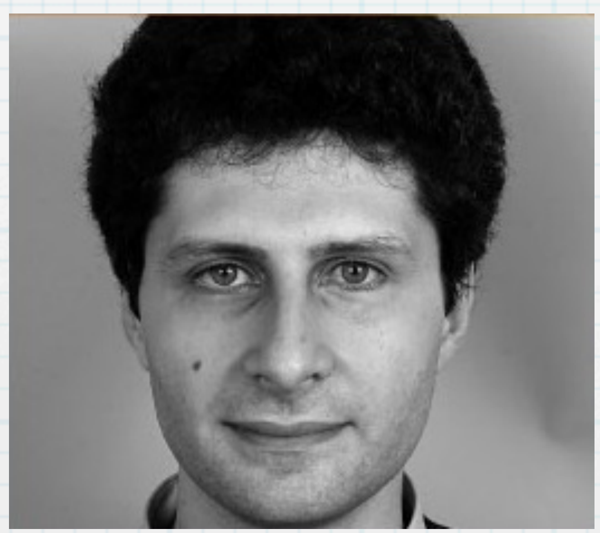
Chiara Macchiavello

Lorenzo Maccone

Massimiliano Sacchi

Paolo Perinotti

Giulio Chiribella

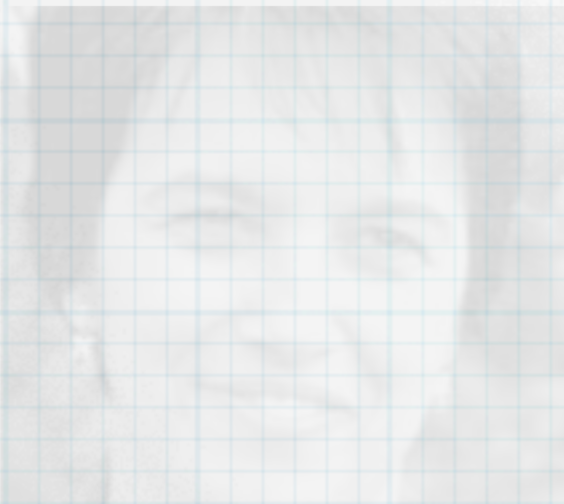


Daniele Magnani

Stefano Facchini

Alessandro Bisio

Theory of Quantum Combs in collaboration with



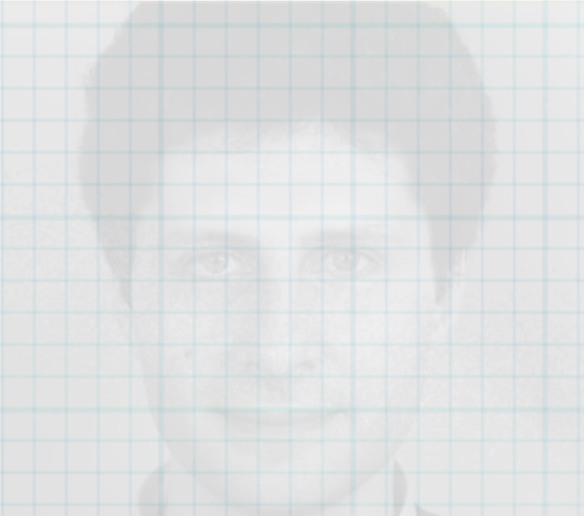
Chiara Macchiavello

Lorenzo Maccone

Massimiliano Sacchi

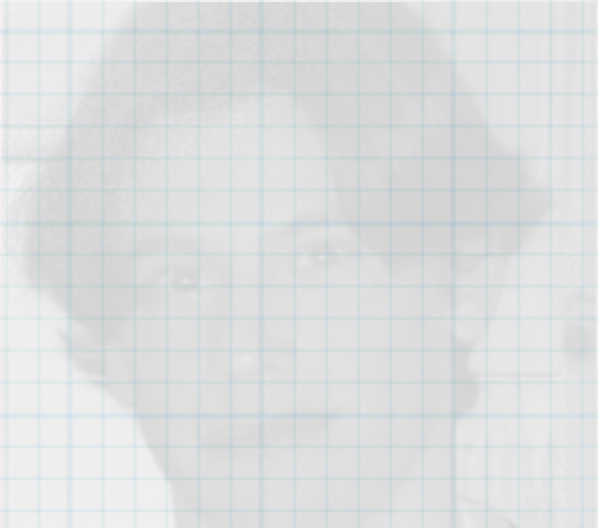
Paolo Perinotti

Giulio Chiribella



Daniele Magnani

Stefano Facchini



Alessandro Bisio

QUit quantum information theory group

Applications to Optimal Q-Tomography and Q-Learning

Chiara Macchiavello

Lorenzo Maccone

Massimiliano Sacchi


Paolo Perinotti


Giulio Chiribella


Daniele Magnani


Stefano Facchini


Alessandro Bisio

Outline

Outline

- New Quantum Estimation Theory, with multiple copies, and optimization of the setup
  - Convex optimization method based on the new notions of quantum comb and quantum tester

Outline

- New Quantum Estimation Theory, with multiple copies, and optimization of the setup
  - Convex optimization method based on the new notions of quantum comb and quantum tester
- Applications:
  - discrimination of unitary operators and of memory channels (quantum oracle-calling algoritms)
  - strategies in quantum protocols, crypto and games
  - quantum-algorithm learning (storing undisclosable unitaries)
  - process-cloning
  - optimal tomography

optimal

Outline

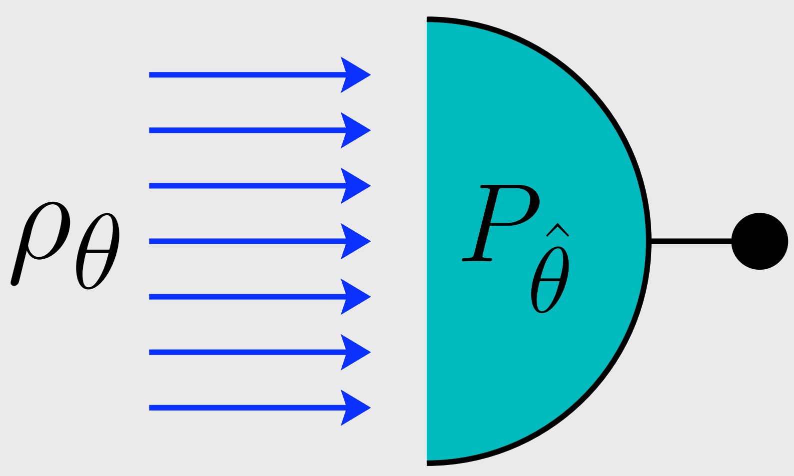
- New Quantum Estimation Theory, with multiple copies, and optimization of the setup
  - Convex optimization method based on the new notions of quantum comb and quantum tester
- Applications:
  - discrimination of unitary operators and of memory channels (quantum oracle-calling algoritms)
  - strategies in quantum protocols, crypto and games
  - quantum-algorithm learning (storing undisclosable unitaries)
  - process-cloning
  - optimal tomography

optimal

Helstrom-Holevo Quantum Estimation Theory

Quantum state ρ_θ parameterized by θ

Problem: estimate θ optimally according to the cost function $C(\theta, \hat{\theta})$



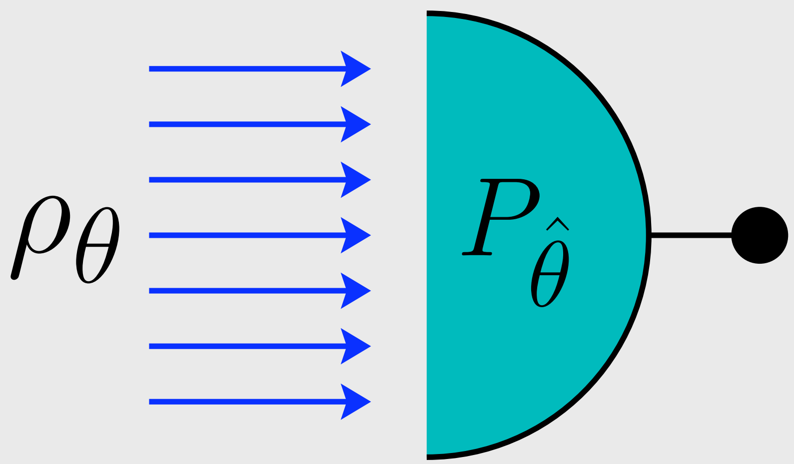
Helstrom-Holevo Quantum Estimation Theory

Quantum state ρ_θ parameterized by θ

Problem: estimate θ optimally according to the cost function $C(\theta, \hat{\theta})$

Mathematical formulation:

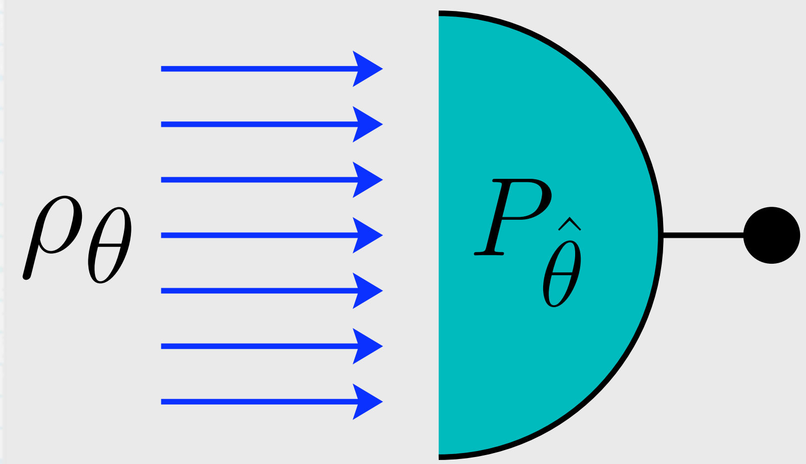
find the optimal POVM $P_{\hat{\theta}}$ minimizing the cost



Helstrom-Holevo Quantum Estimation Theory

Practically interesting situation (e.g. for the phase of an e.m. mode):

$$\boxed{\theta \Longrightarrow \rho_\theta = U_\theta \rho U_\theta^\dagger}$$



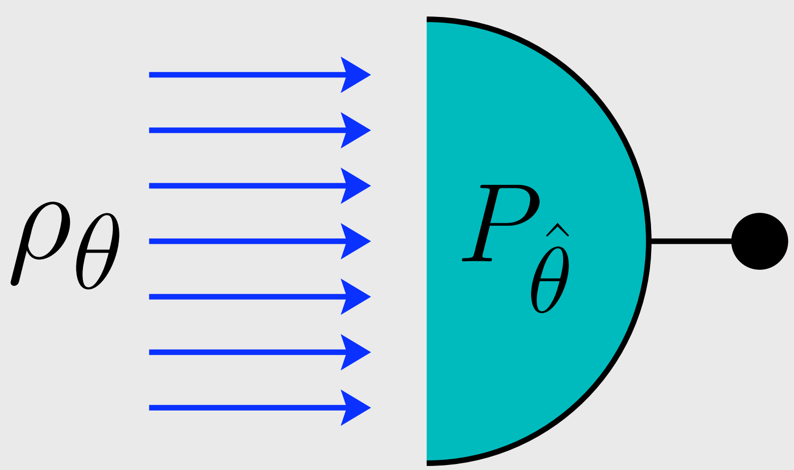
Helstrom-Holevo

Quantum Estimation Theory

Practically interesting situation
(e.g. for the phase of an e.m. mode):

$$\boxed{\theta \Longrightarrow \rho_\theta = U_\theta \rho U_\theta^\dagger}$$

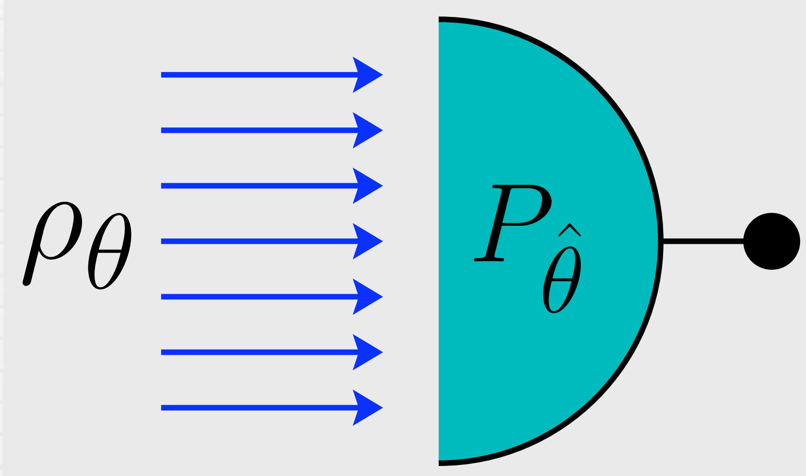
Then you want also to optimize ρ



Helstrom-Holevo Quantum Estimation Theory

Practically interesting situation (e.g. for the phase of an e.m. mode):

$$\boxed{\theta \Longrightarrow \rho_\theta = U_\theta \rho U_\theta^\dagger}$$



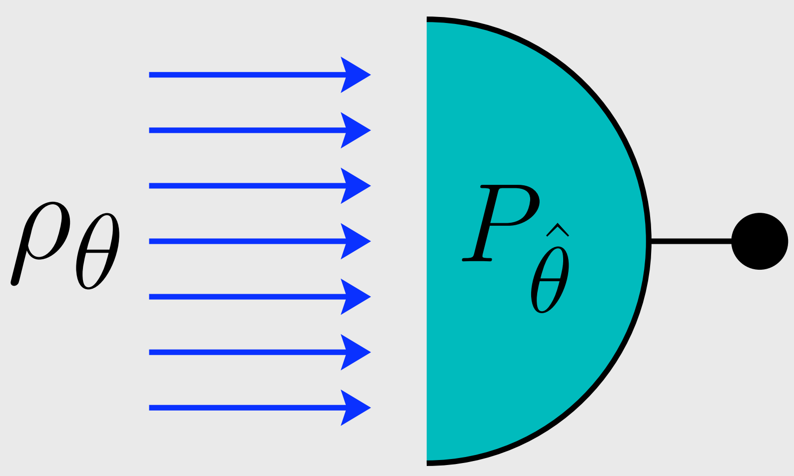
Then you want also to optimize ρ

The optimal POVM for estimating θ depends on ρ

Helstrom-Holevo Quantum Estimation Theory

Practically interesting situation
(e.g. for the phase of an e.m. mode):

$$\boxed{\theta \Longrightarrow \rho_\theta = U_\theta \rho U_\theta^\dagger}$$



Then you want also to optimize ρ

The optimal POVM for
estimating θ depends on ρ

Interesting situation: the parameter to be estimated
is encoded on a transformation---not on the state!

QUit quantum information theory group

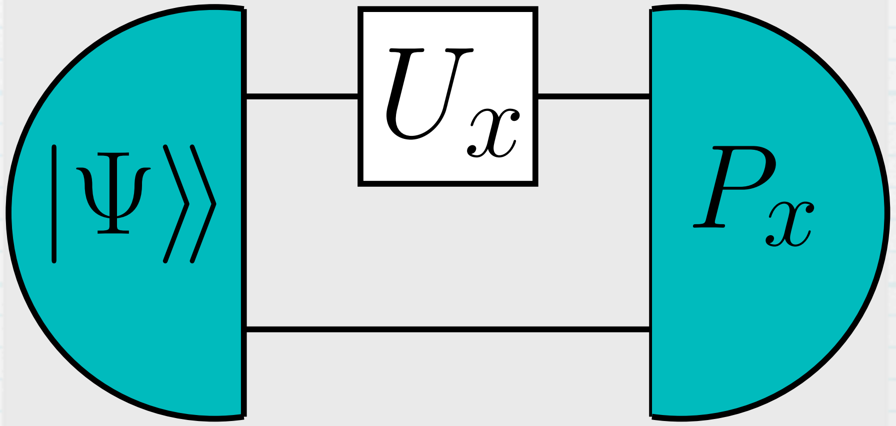
Quantum Estimation Theory

Problem: estimate x parameterizing the (unitary) transformation U_x optimally according to the cost function

Quantum Estimation Theory

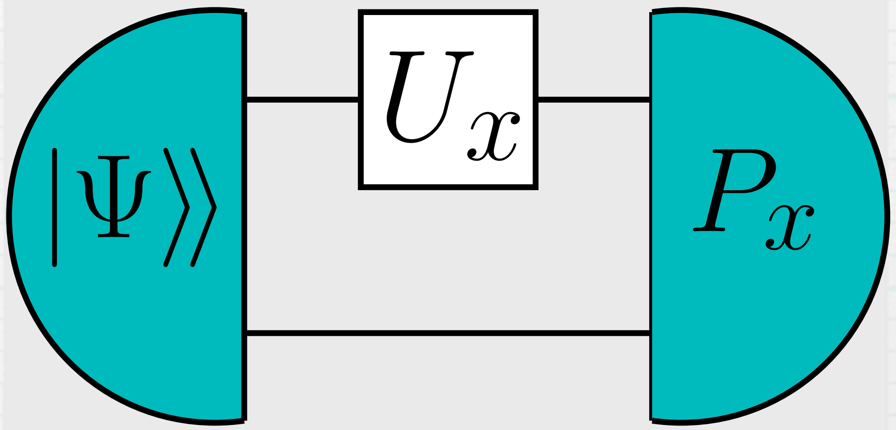
Problem: estimate x parameterizing the (unitary) transformation U_x optimally according to the cost function

Lesson that we learned from entanglement:



Quantum Estimation Theory

Problem: estimate x parameterizing the (unitary) transformation U_x optimally according to the cost function



Lesson that we learned from entanglement:

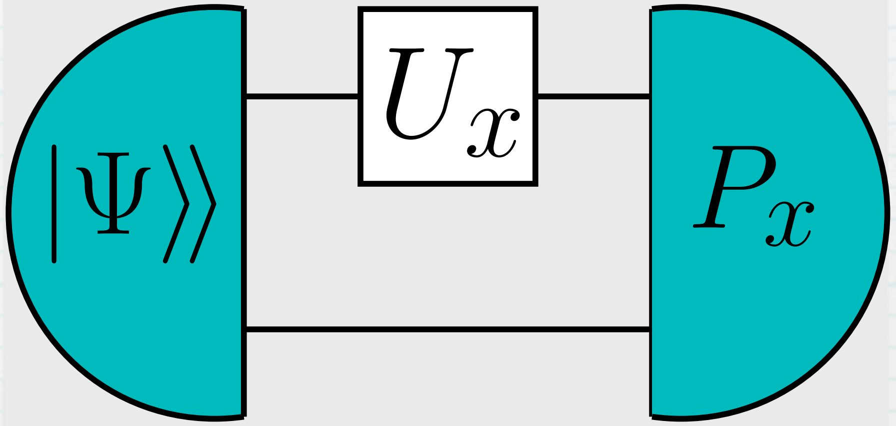
Find the optimal entangled state $|\Psi\rangle\rangle$ (with an any possible ancilla) along with the optimal joint POVM P_x

Quantum Estimation Theory

Problem: estimate x parameterizing the (unitary) transformation U_x optimally according to the cost function

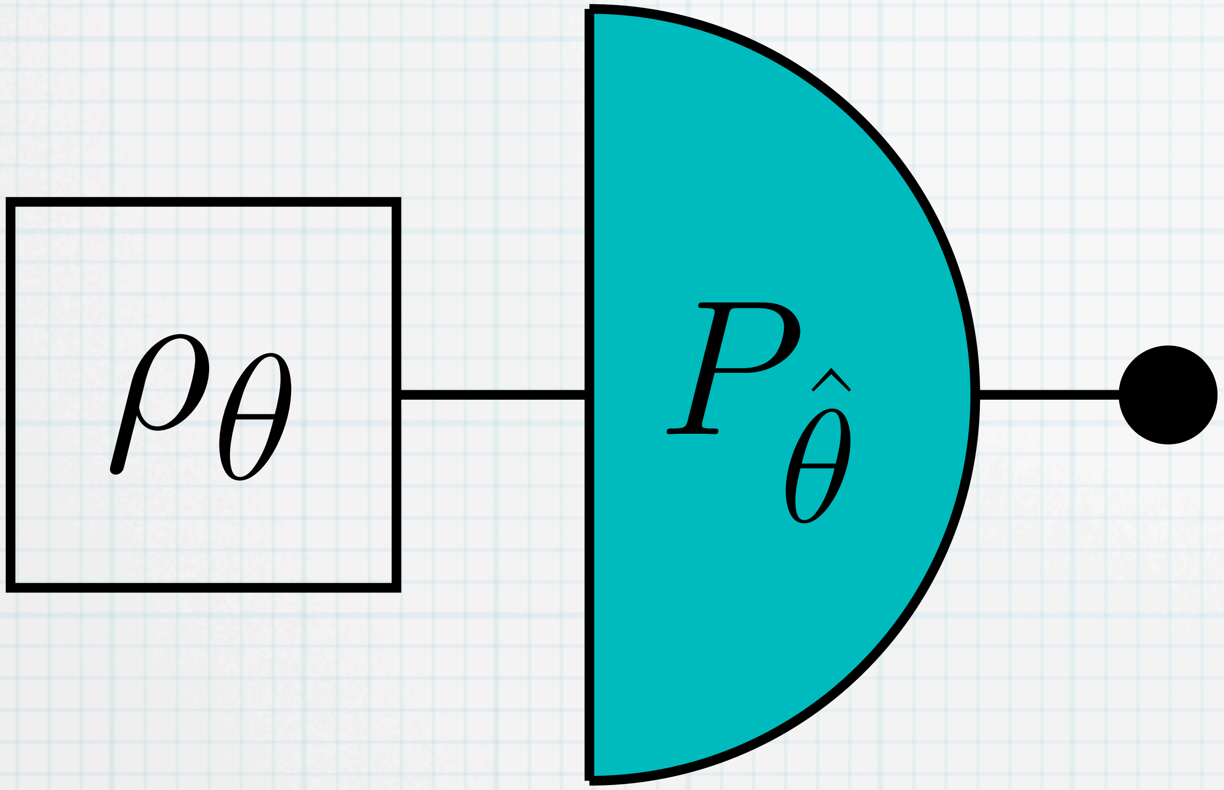
Lesson that we learned from entanglement:

Find the optimal entangled state $|\Psi\rangle\rangle$ (with an any possible ancilla) along with the optimal joint POVM P_x



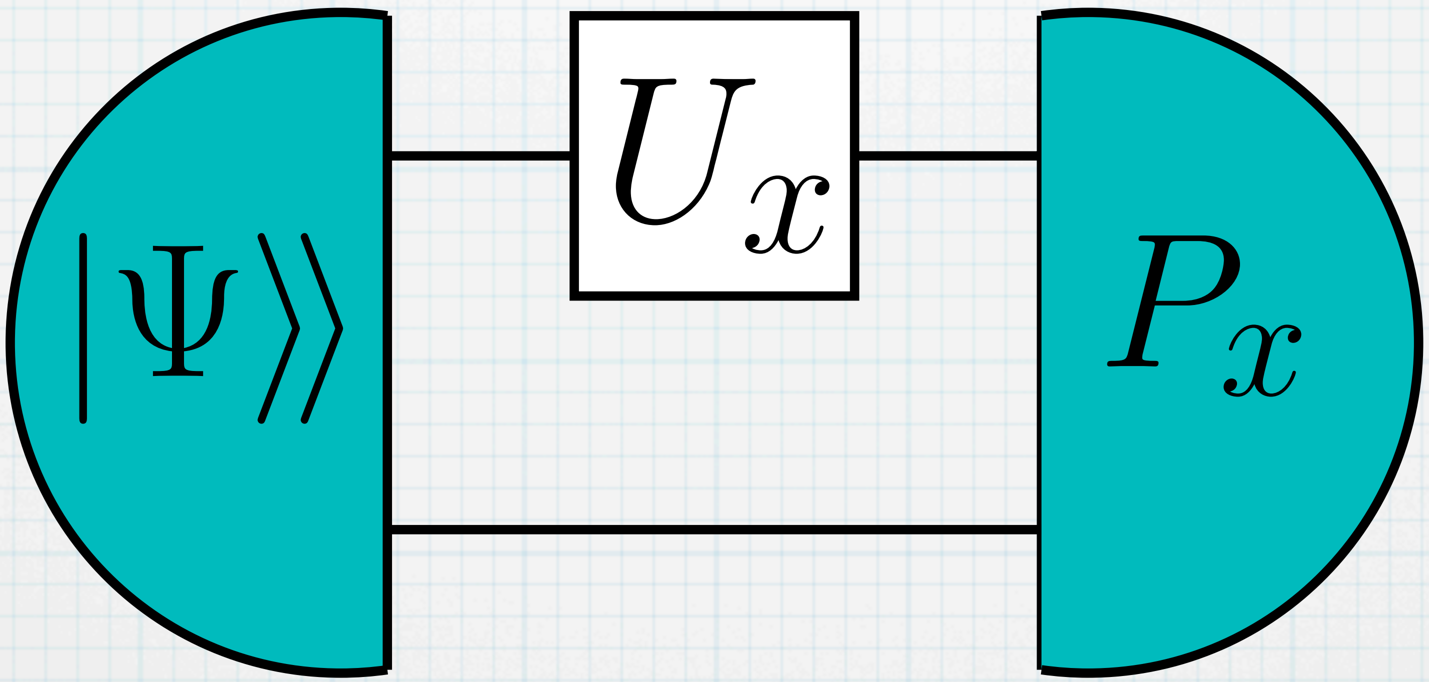
For the phase no need of entanglement (we were lucky!)

Quantum Estimation Theory

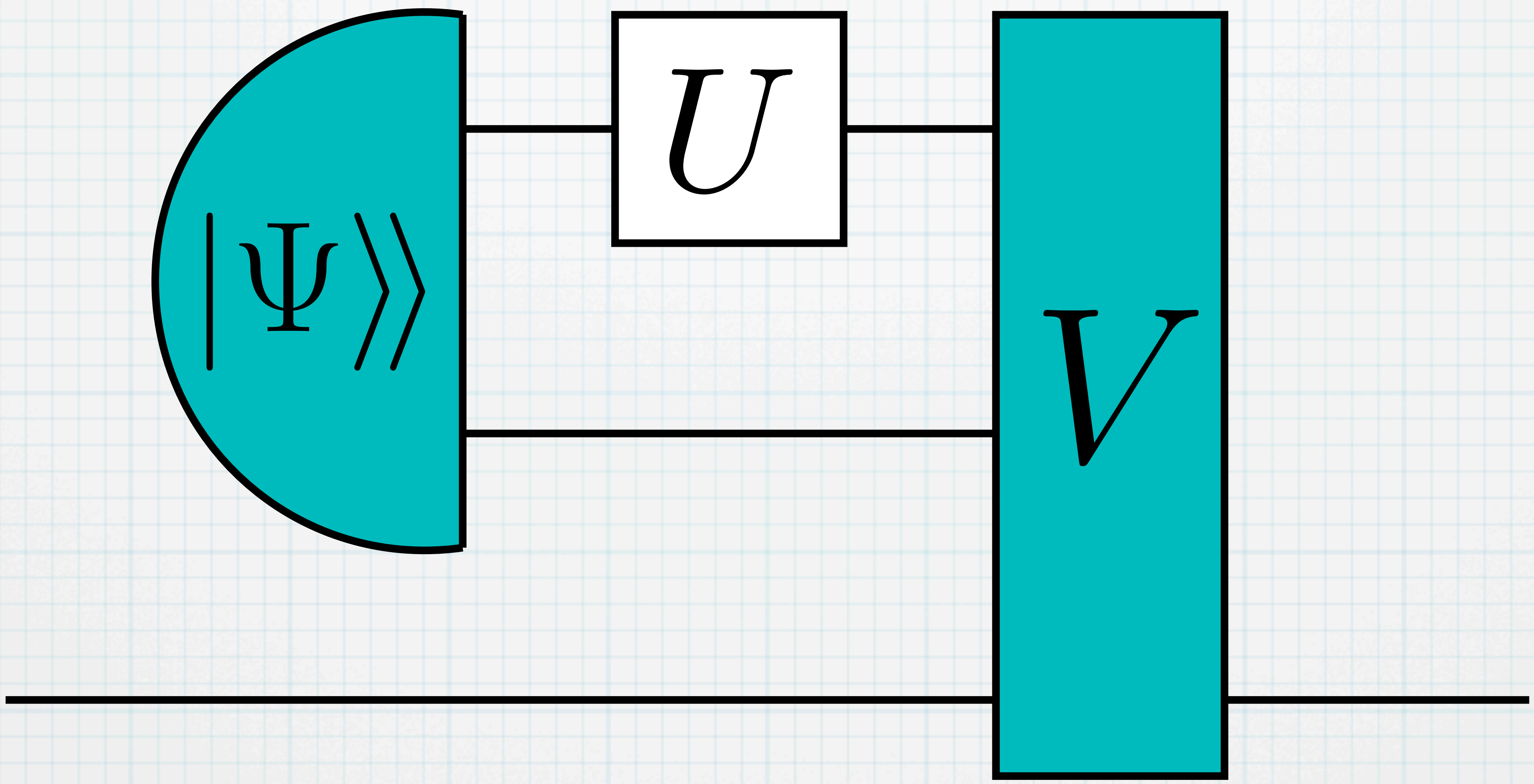


Quantum Estimation Theory

New scheme

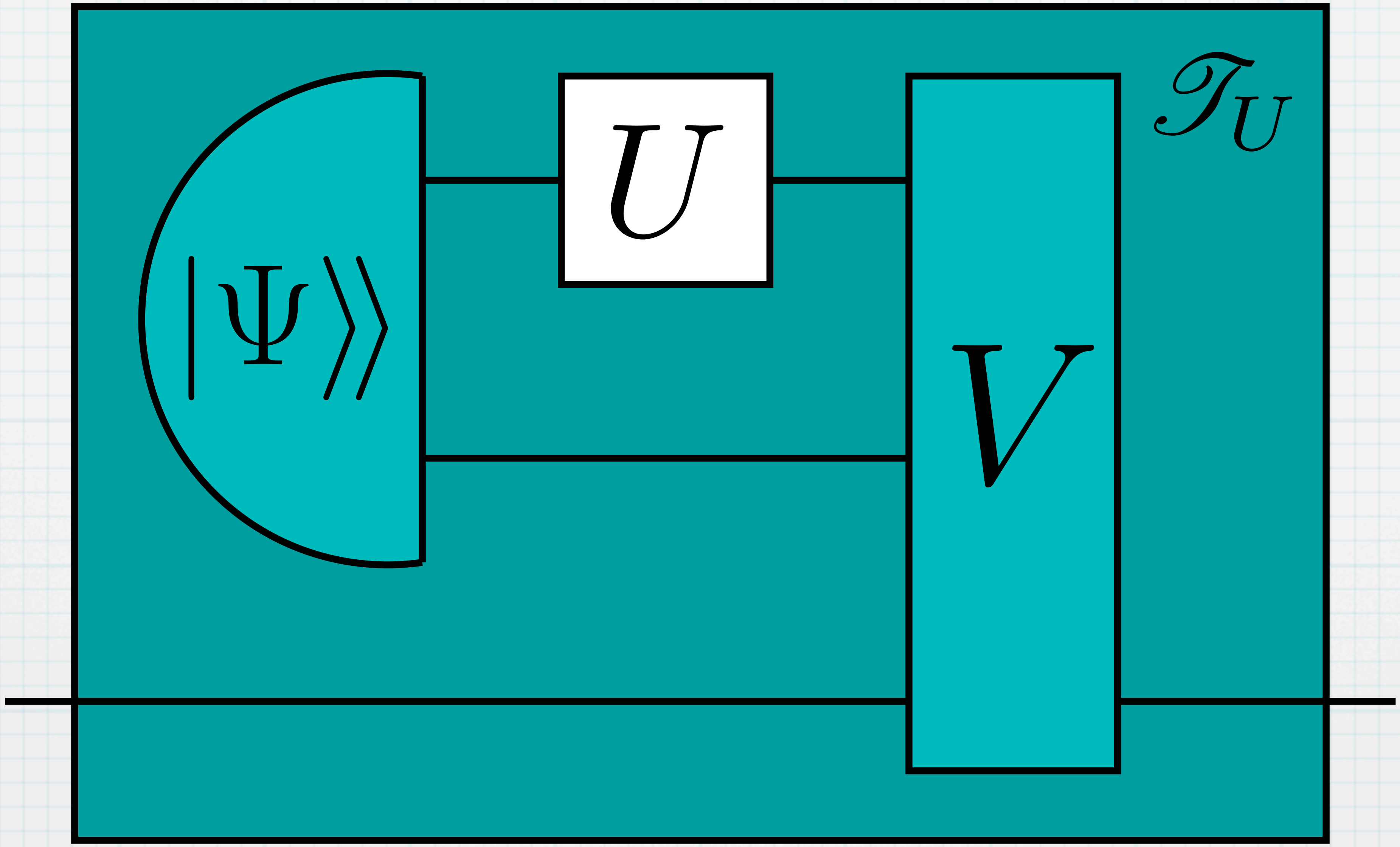


Quantum Feedback



- quantum feedback: perform a transformation $\mathscr{T}_U$ on a system which depends on an unknown unitary transformation U occurring on a (generally different) system (e.g. reference-frames realignment).

Quantum Feedback



- quantum feedback: perform a transformation $\mathscr{T}_U$ on a system which depends on an unknown unitary transformation U occurring on a (generally different) system (e.g. reference-frames realignment).

Multiple copies

- For parameter estimation: repeat the estimation N times, gaining a precision factor $\sqrt{N}$

Multiple copies

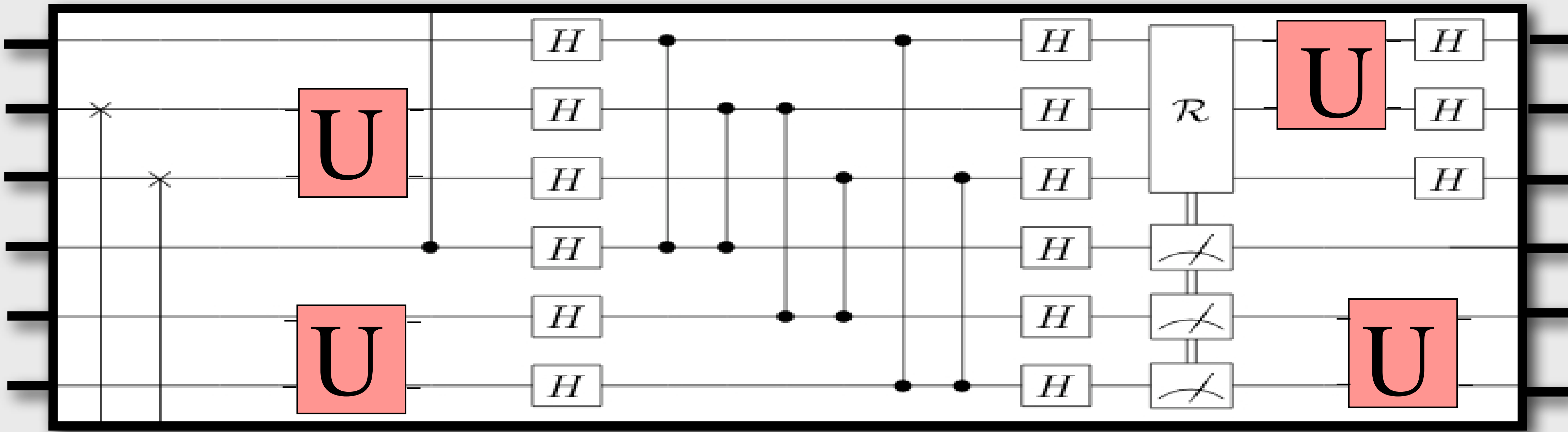
- For parameter estimation: repeat the estimation N times, gaining a precision factor $\sqrt{N}$
- However, you better use a coherent strategy, in which you perform a joint POVM

Multiple copies

- For parameter estimation: repeat the estimation N times, gaining a precision factor $\sqrt{N}$
- However, you better use a coherent strategy, in which you perform a joint POVM
- and you want to do the same for the quantum feedback

What is the best that you can do?

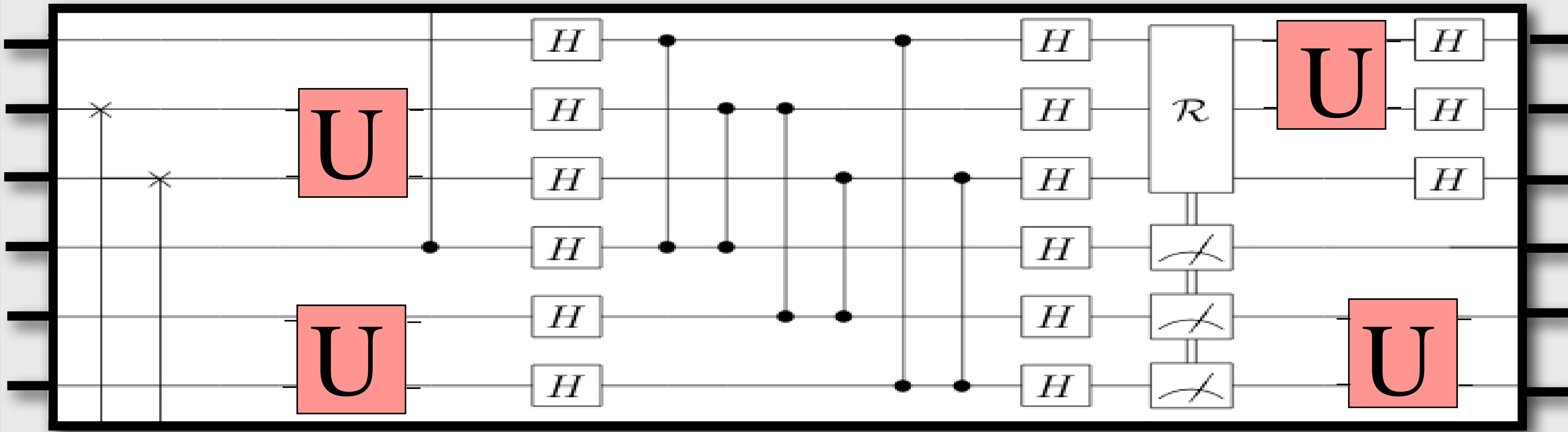
Use a Quantum Board!



General scheme: put the copies of the unknown unitary in a suitable quantum circuit which performs the desired transformation/estimation.

QUit quantum information theory group

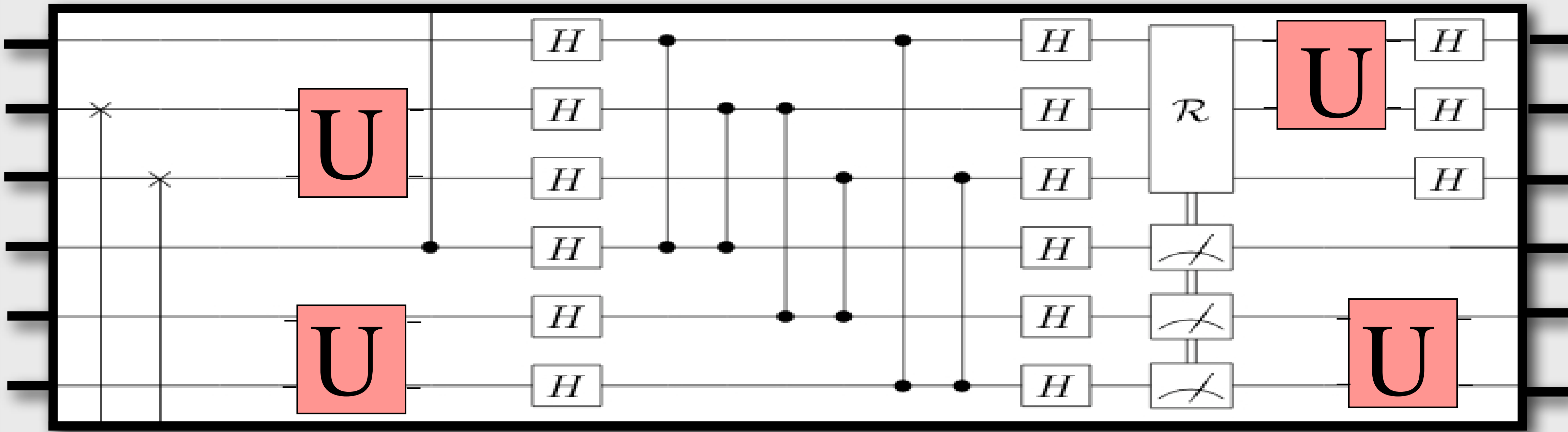
Use a Quantum Board!



General scheme: put the copies of the unknown unitary in a suitable quantum circuit which performs the desired transformation/estimation.

Quantum circuit board: input and output are themselves circuits that are slotted into the board.

Use a Quantum Board!



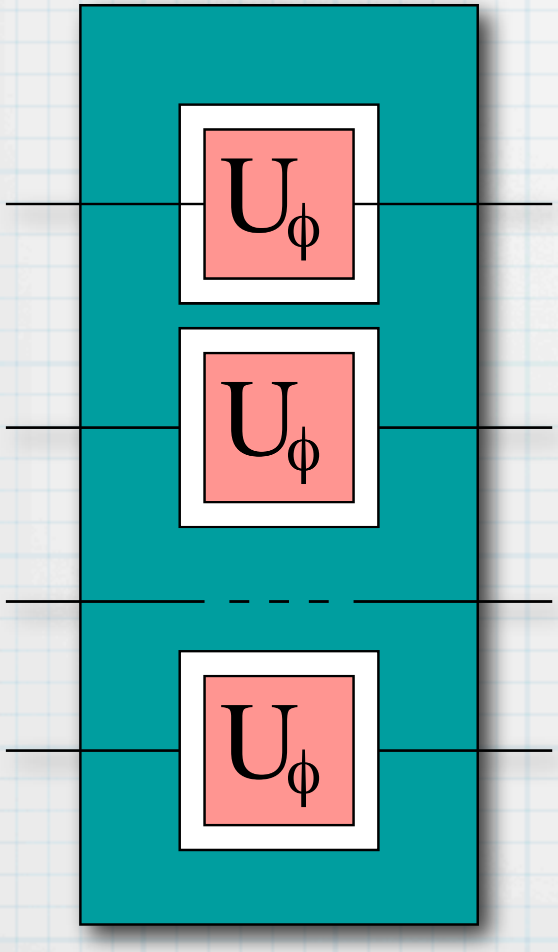
Optimize the quantum circuit board for all possible dispositions of the slots

QUit quantum information theory group

It looks a difficult problem ...

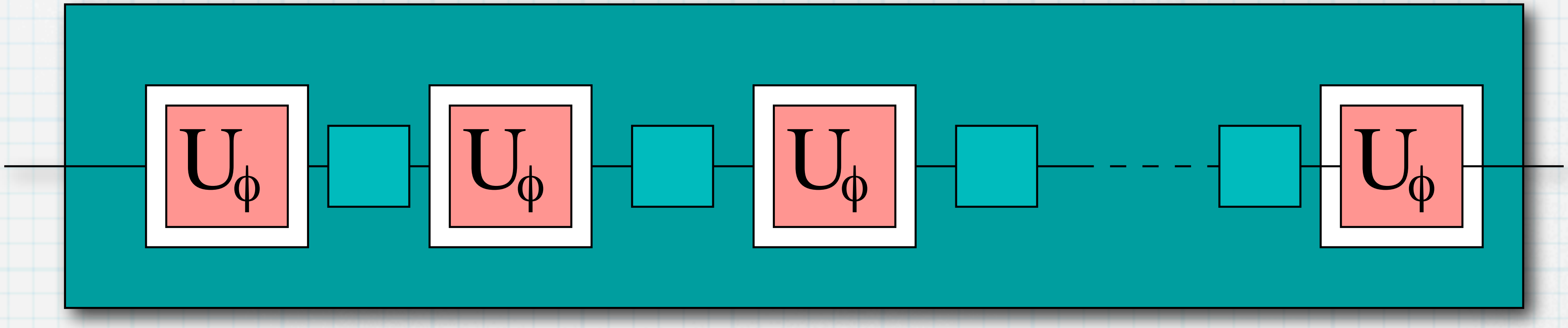
For example: what is the optimal board for phase estimation?

For example: what is the optimal board for phase estimation?

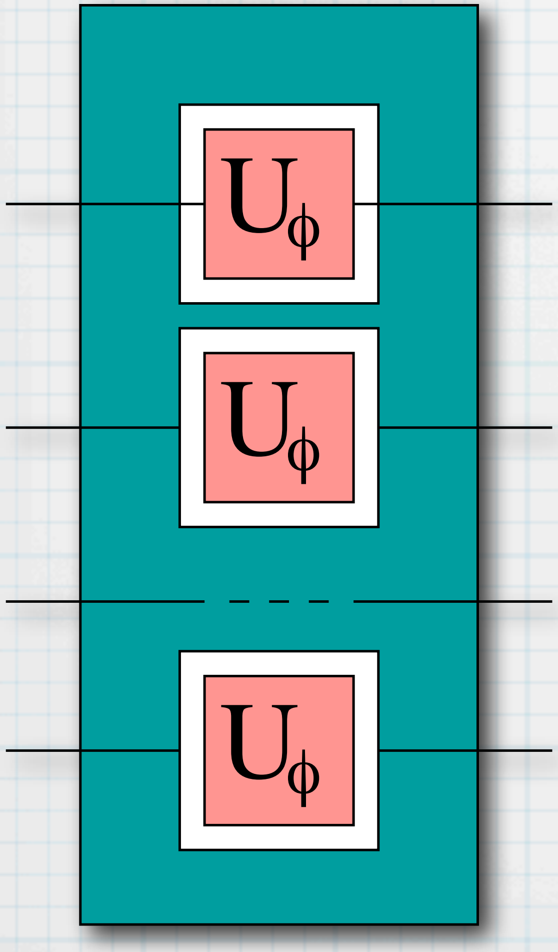


In parallel over a joint entangled state?

For example: what is the optimal board for phase estimation?

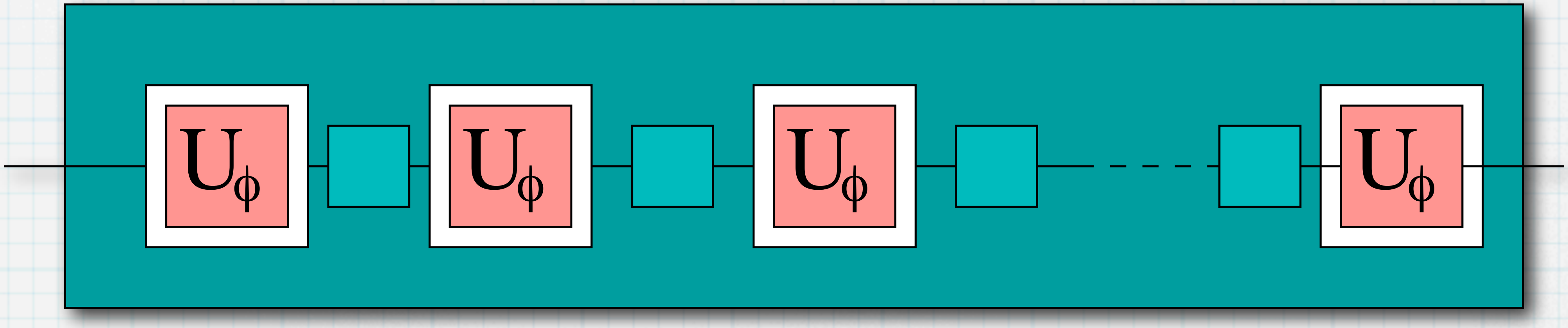


In sequence intercalated by some unitary?

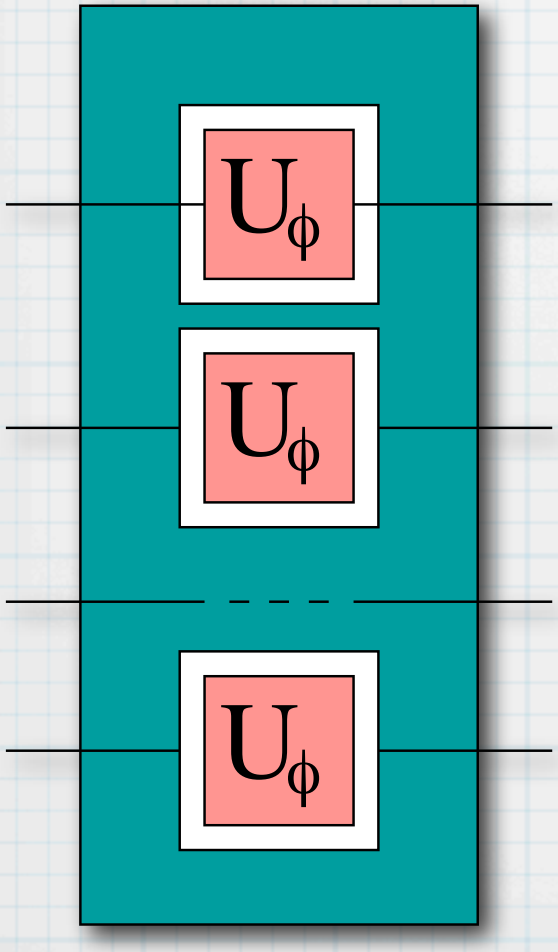


In parallel over a joint entangled state?

For example: what is the optimal board for phase estimation?



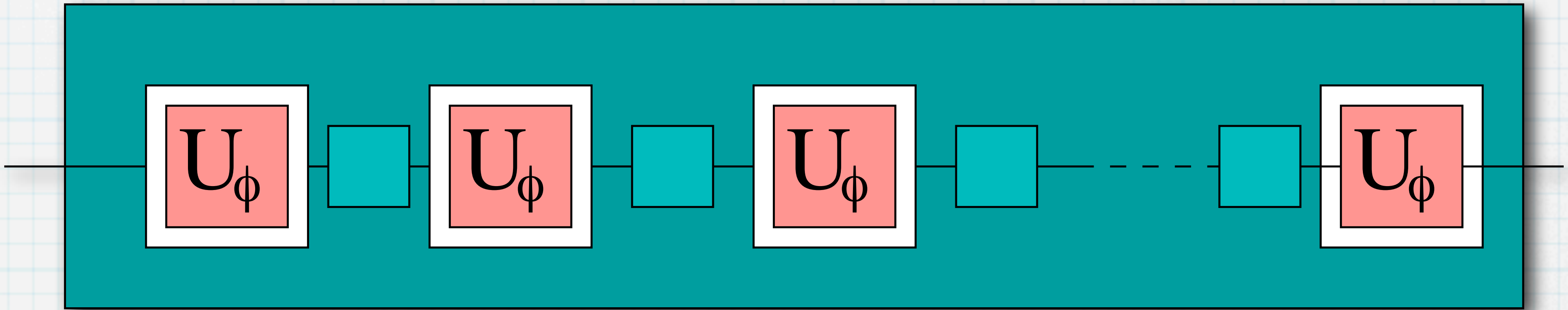
In sequence intercalated by some unitary?



In parallel over a joint entangled state?

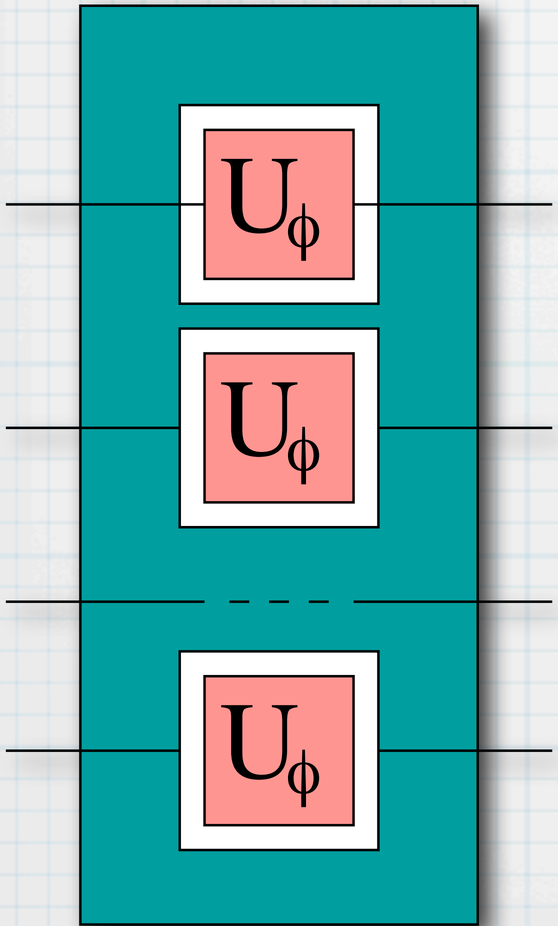
Asymptotically: same sensitivity [Giovannetti, LLoyd, Maccone, PRL 96, 010401 (2006)]

For example: what is the optimal board for phase estimation?



In sequence intercalated by some unitary?

For unitary discrimination: [Duan, Feng, Ying, PRL 98, 100503 (2007)]



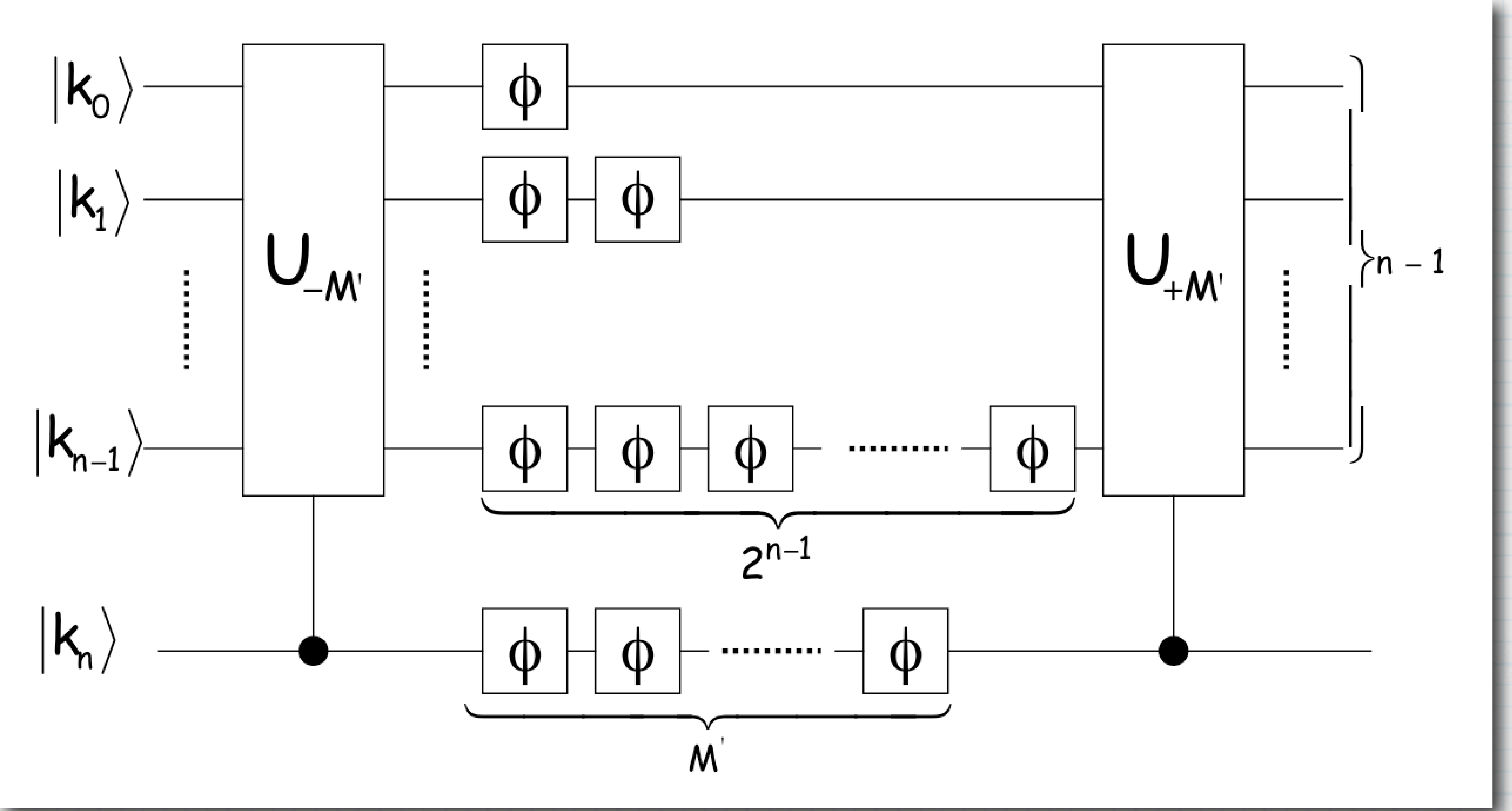
In parallel over a joint entangled state?

For unitary discrimination: G.M.D'Ariano, P. Lo Presti, M. Paris, PRL 87, 270404 (2001); A. Acín, E. Jané, and G. Vidal, Phys. Rev. A 64, 050302 (2001)

Asymptotically: same sensitivity [Giovannetti, LLoyd, Maccone, PRL 96, 010401 (2006)]

For example: what is the optimal board for phase estimation?

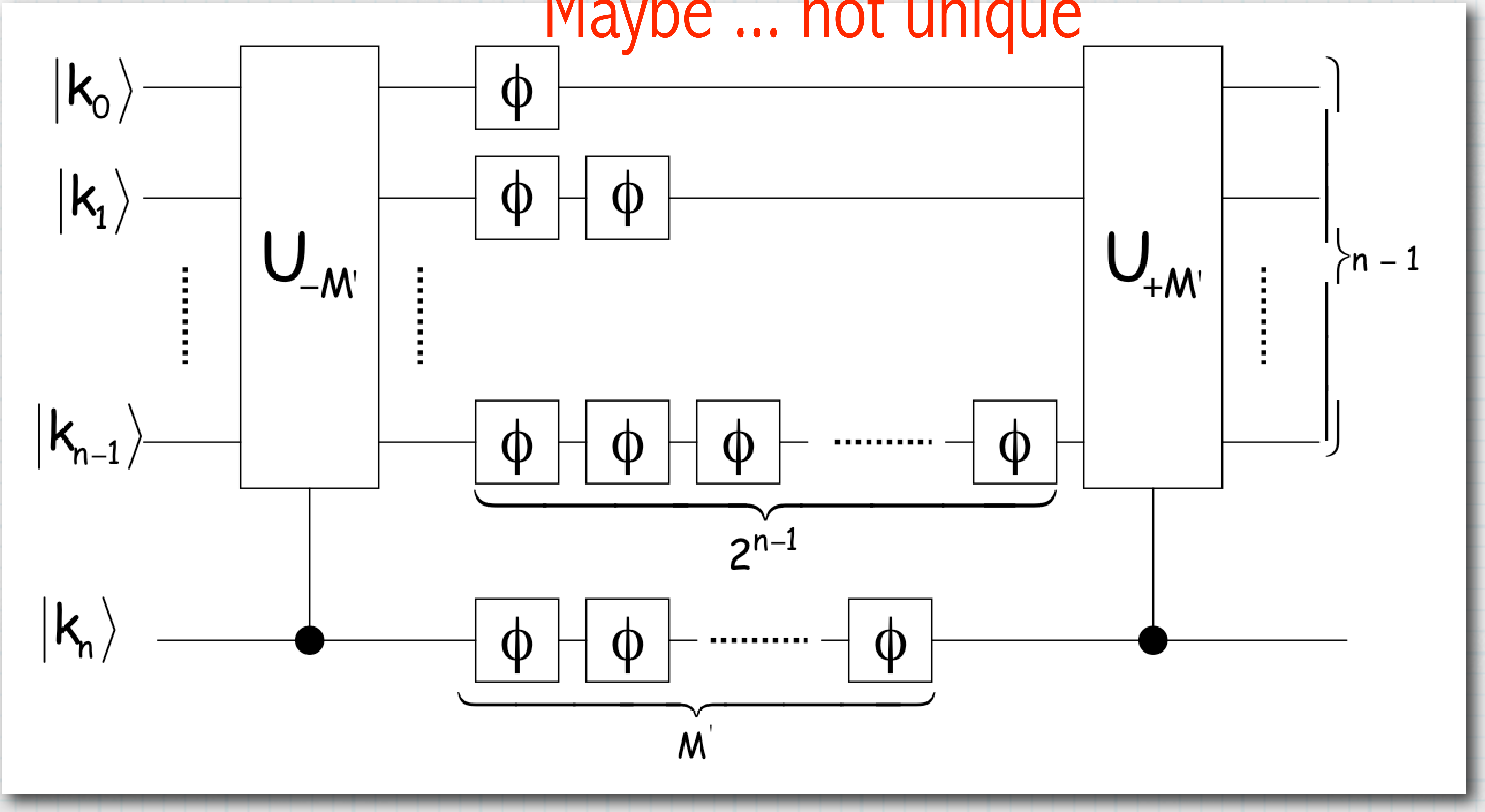
An optimal board architecture [van Dam, D'Ariano, Ekert, Macchiavello, Mosca, PRL 98, 090501 (2007)]



For example: what is the optimal board for phase estimation?

An optimal board architecture [van Dam, D'Ariano, Ekert, Macchiavello, Mosca, PRL 98, 090501 (2007)]

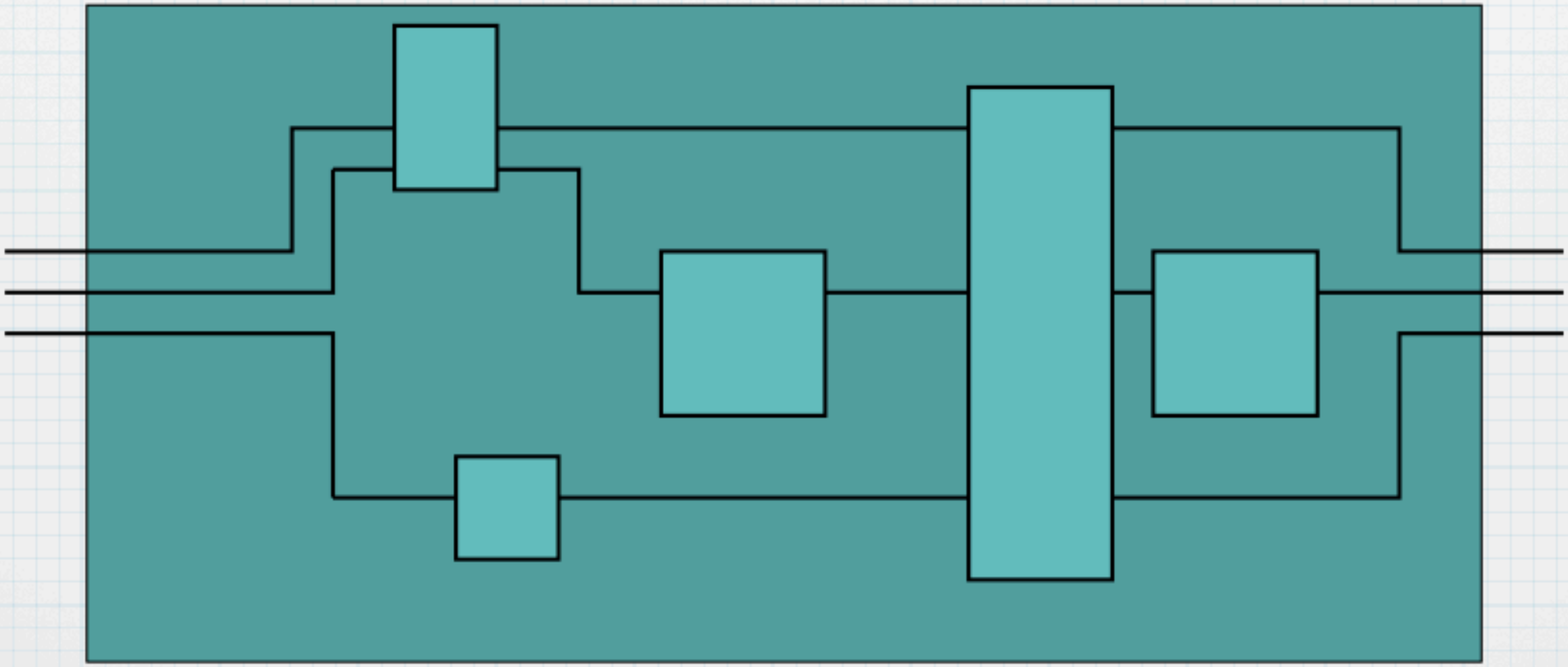
Maybe ... not unique



What is the mathematical formulation of the problem?

Quantum Channel

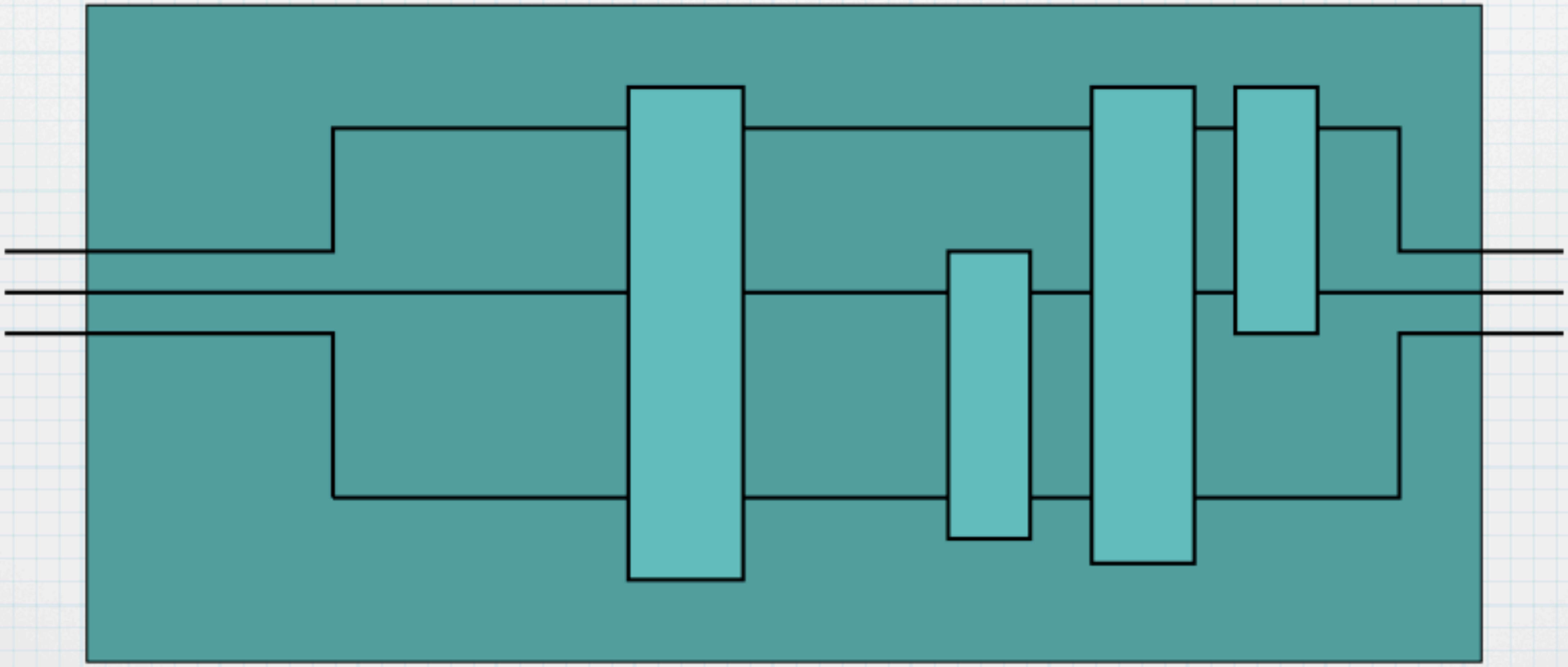
It can be regarded as an equivalence class of quantum circuits performing the same input-output transformation ...



Quantum Channel

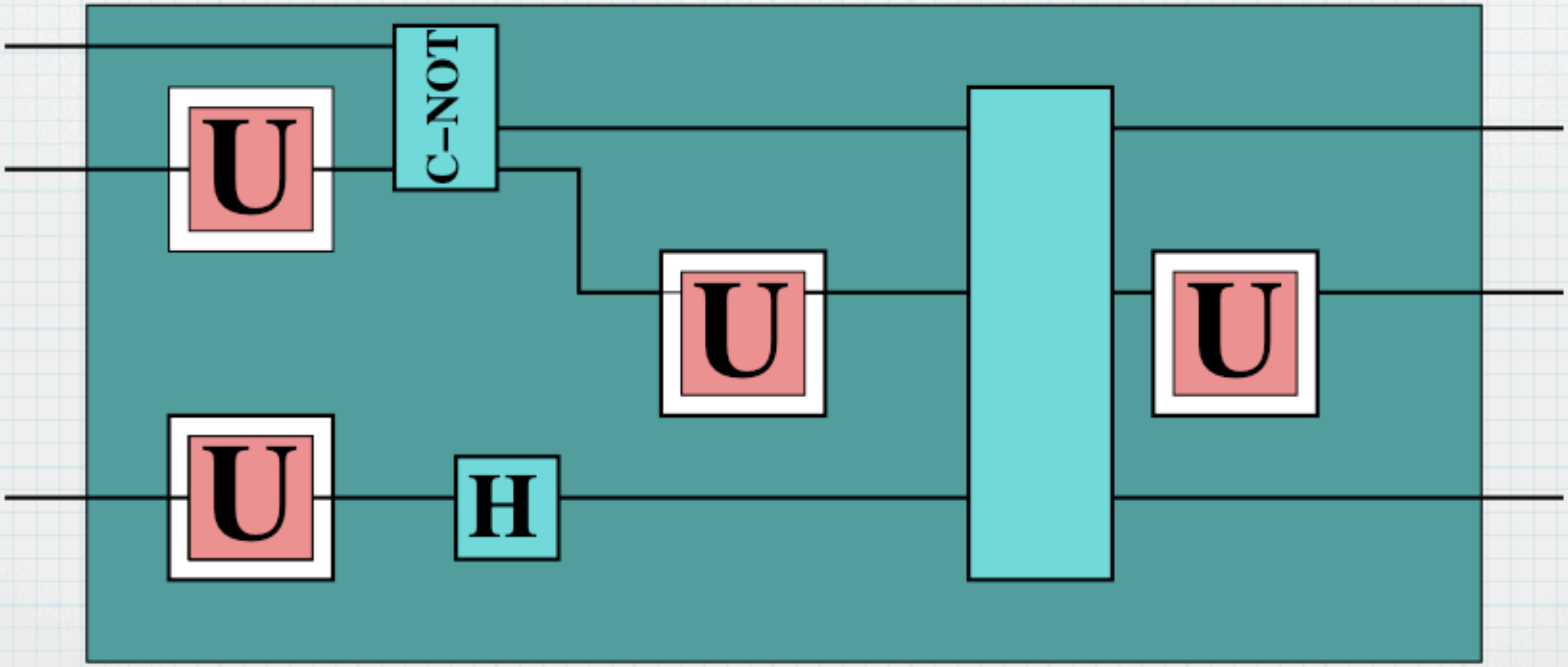
It can be regarded as an equivalence class of quantum circuits performing the same input-output transformation ...

For a channel the input and the output are states



Quantum Board

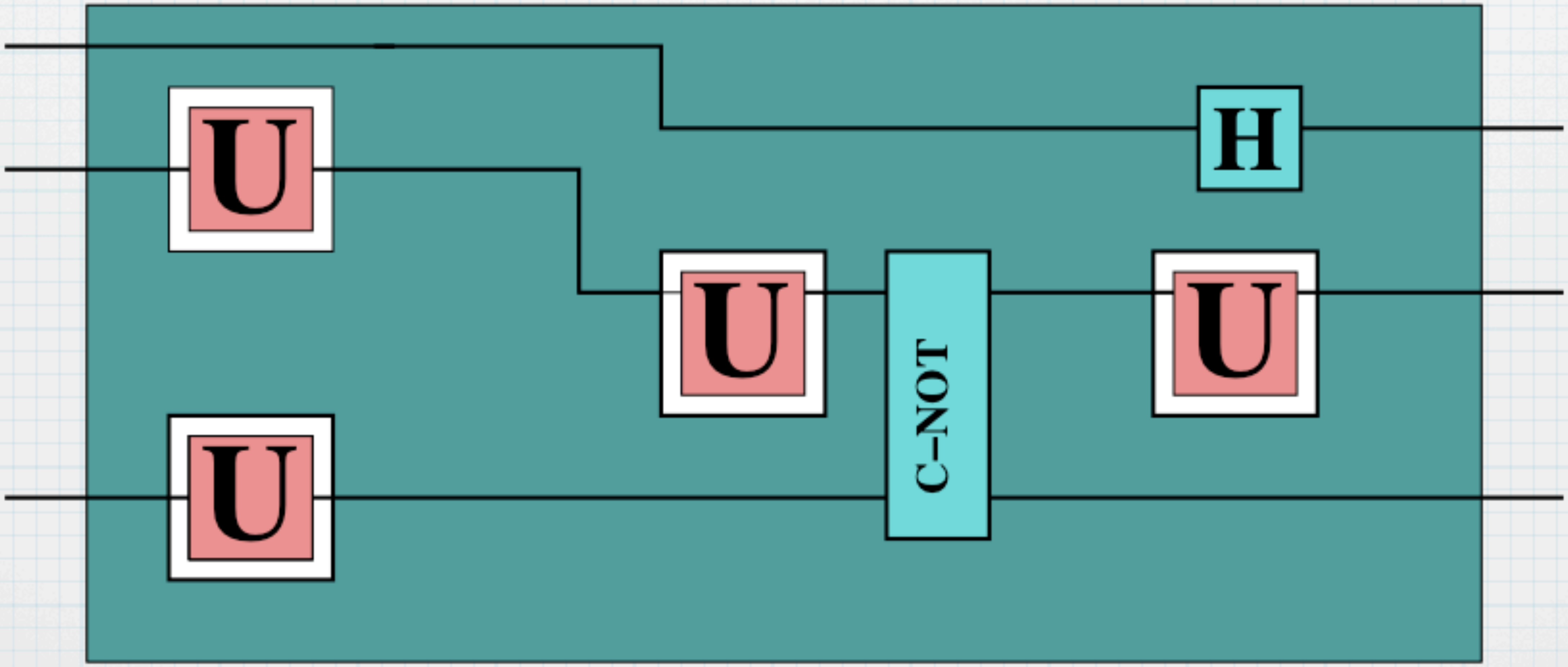
Equivalence class of quantum circuits boards performing the same overall input-output transformation ...



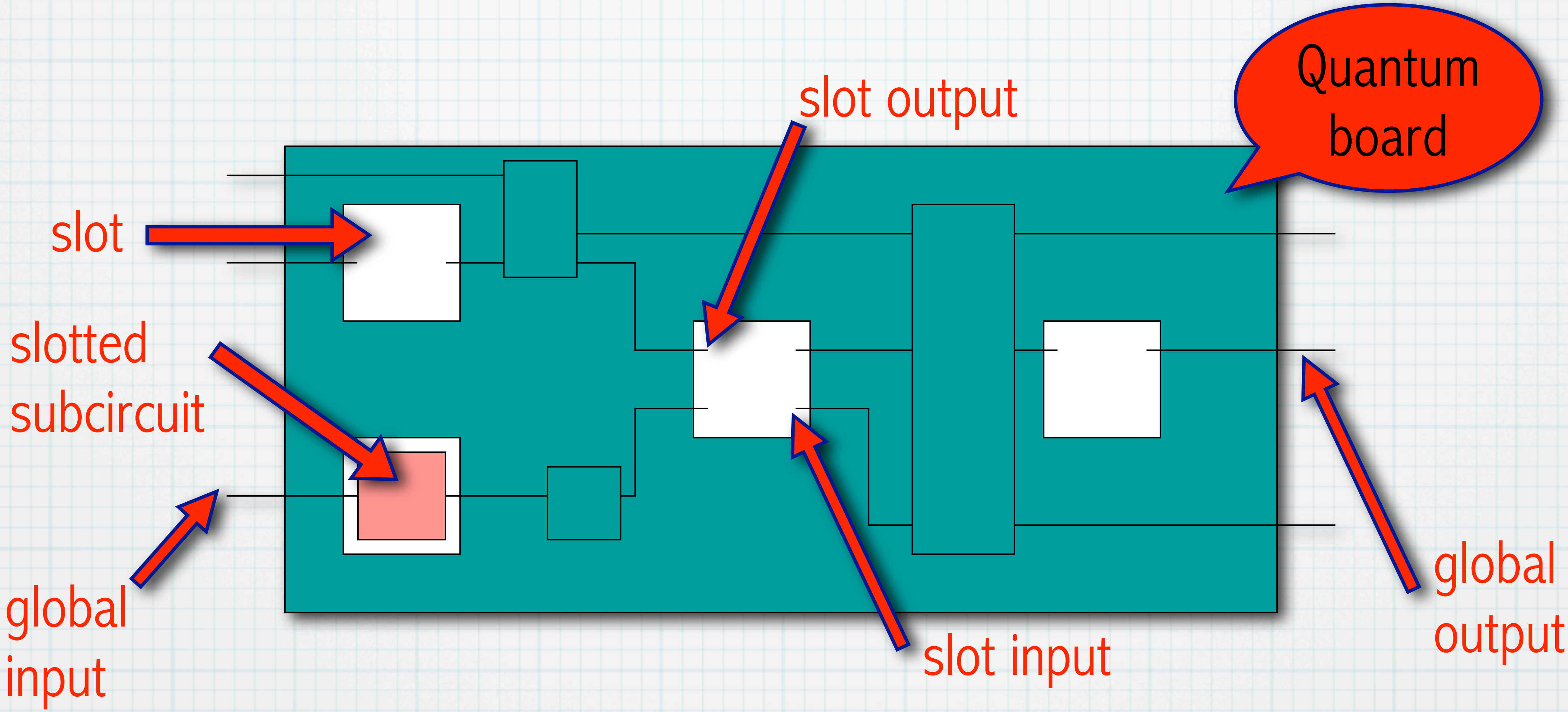
Quantum Board

Equivalence class of quantum circuits boards performing the same overall input-output transformation ...

But now, the input and the output are transformations



Quantum Board

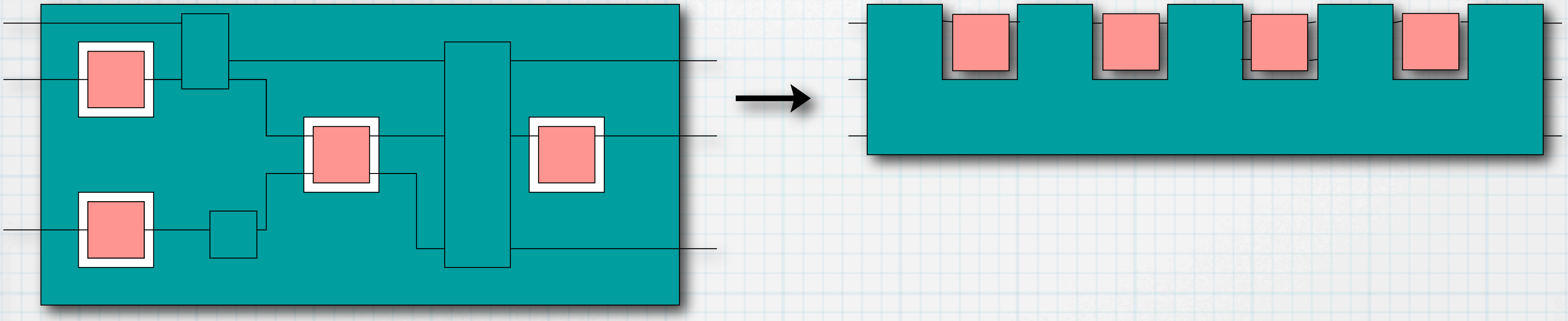


Problem: what is the optimal board for given slots achieving a global input/output transformation optimally according to a given cost function?

Quantum Combs

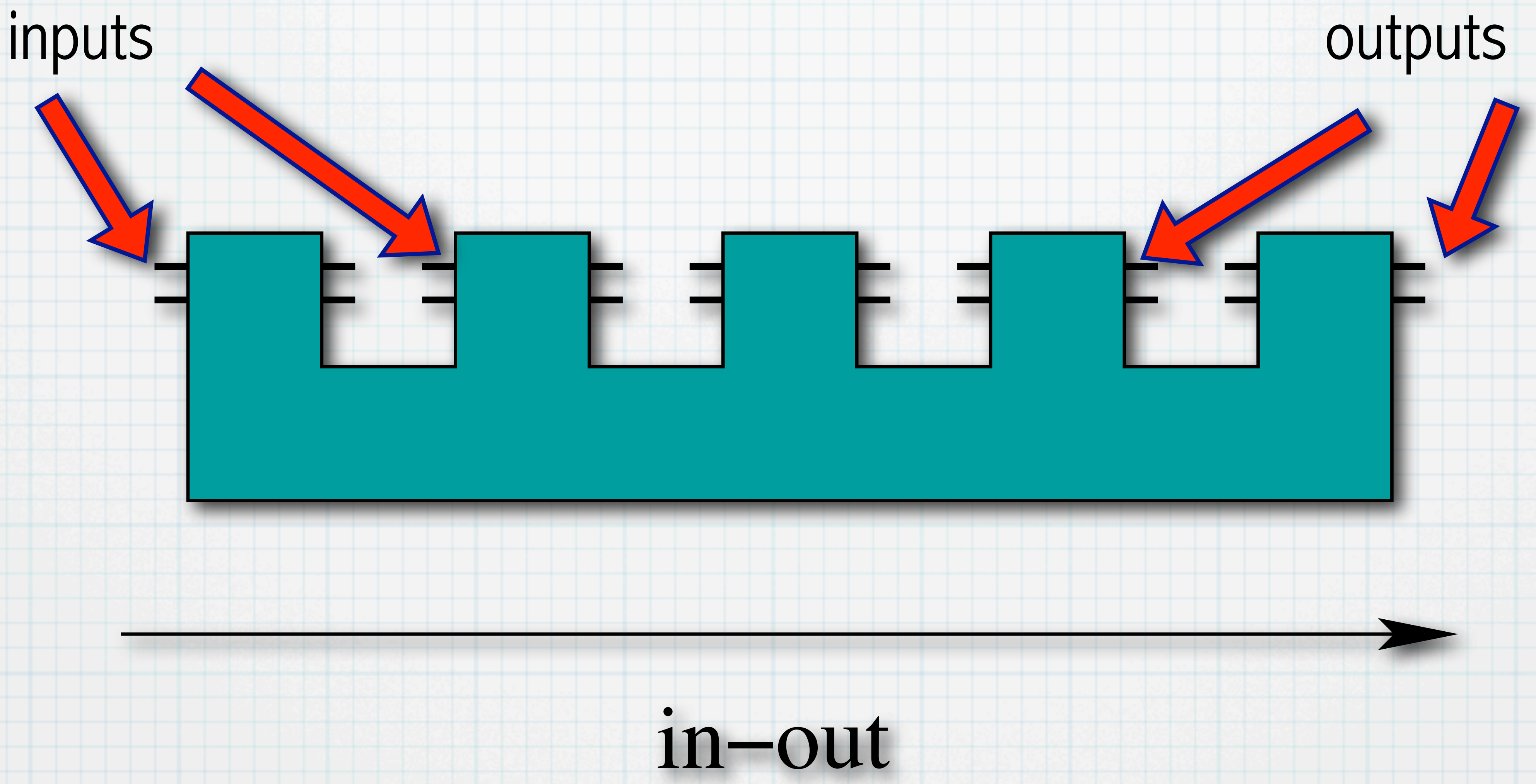
G.Chiribella, G.M.D'Ariano, P.Perinotti, PRL 101 060401 (2008)

All circuits-boards can be reshaped in form of "combs", with an ordered sequence of slots, each between two successive teeth



Quantum Combs

G.Chiribella, G.M.D'Ariano, P.Perinotti, PRL 101 060401 (2008)

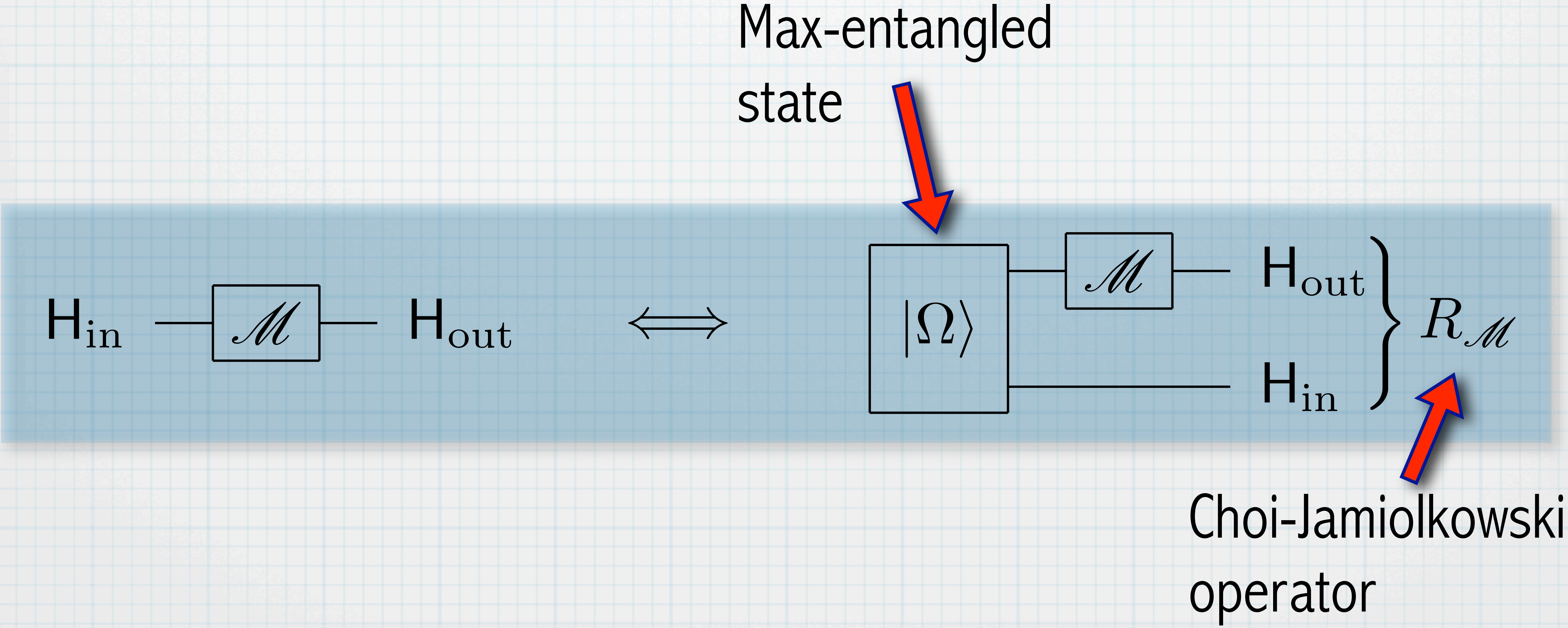


Pins = quantum systems with generally variable dimensions

How do we describe a quantum comb mathematically?

Channel: Choi representation

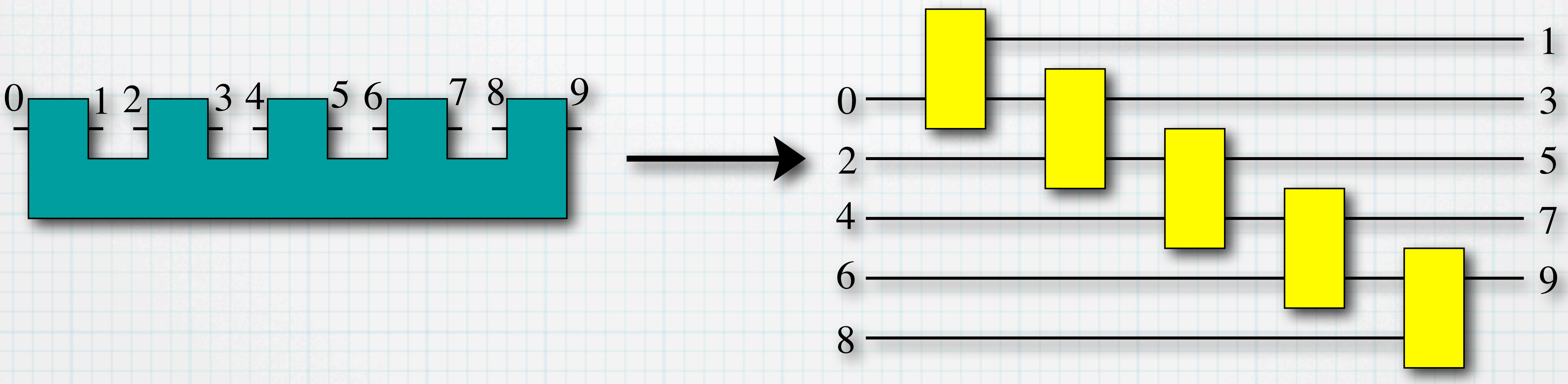
Mathematically the input-output transformation operated by a quantum circuit is a CP map, and is in one-to-one correspondence with a positive operator called "Choi-Jamiolkowski operator"---the output state of the map applied locally to a maximally entangled state.



PRL 101 060401 (2008)

Causal networks

The quantum comb is equivalent to a causal network with all inputs on the left and all outputs on the right

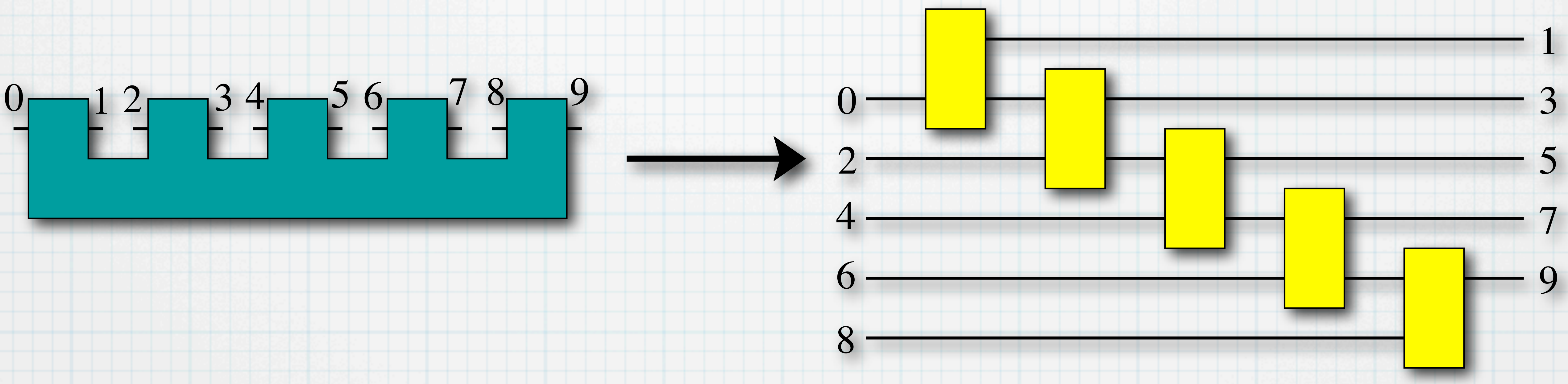


QUit quantum information theory group

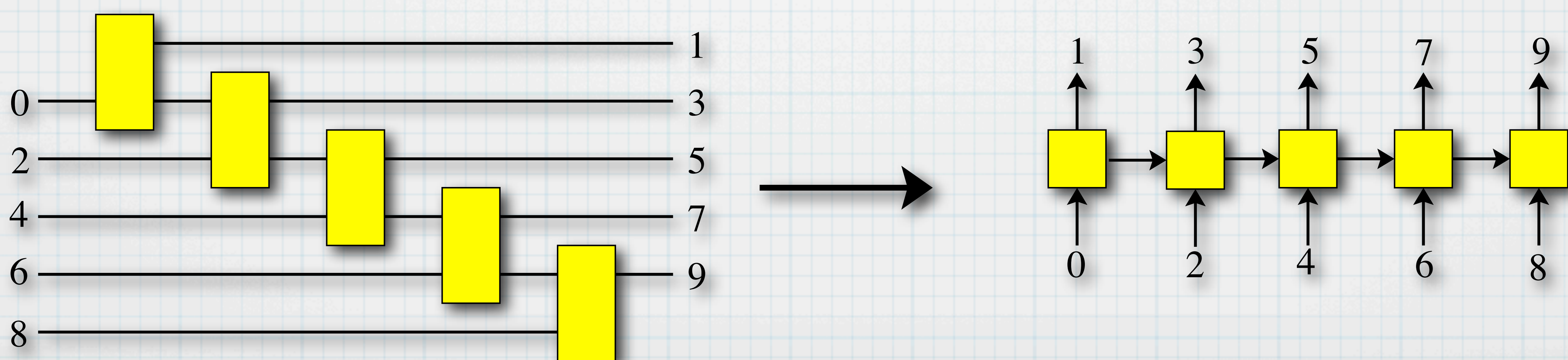
PRL 101 060401 (2008)

Causal networks

The quantum comb is equivalent to a causal network with all inputs on the left and all outputs on the right



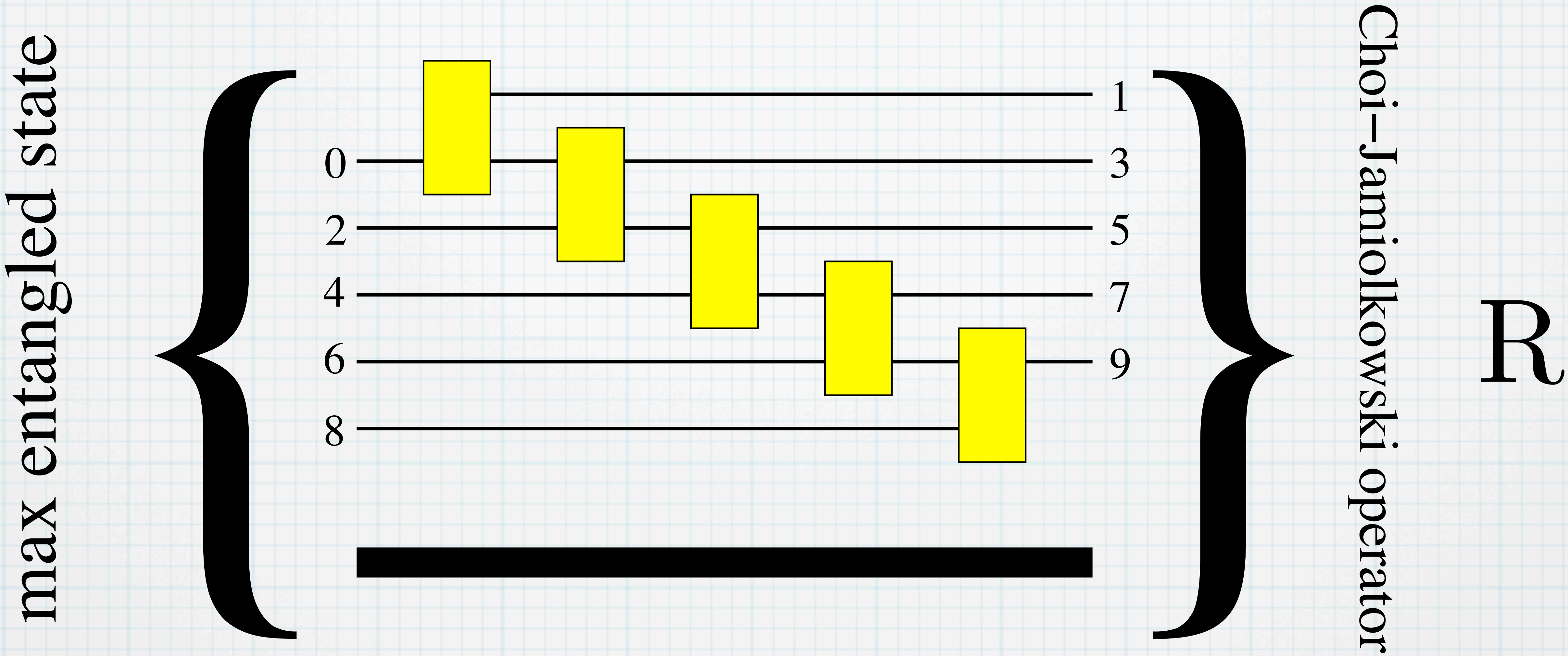
The causal network is also equivalent to the stack of memory channels



QUIT quantum information theory group

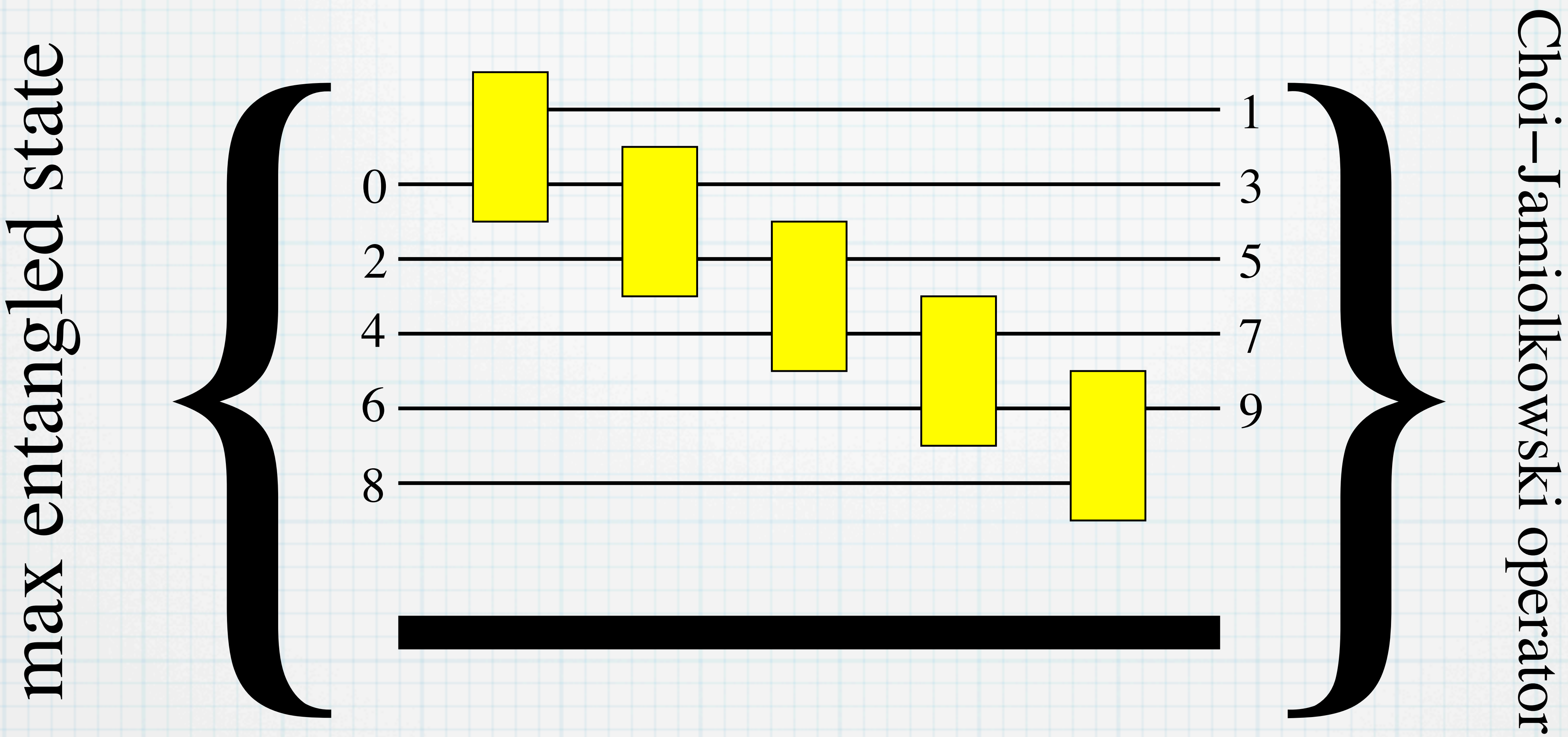
PRL 101 060401 (2008)

Choi representation



PRL 101 060401 (2008)

Choi representation



R

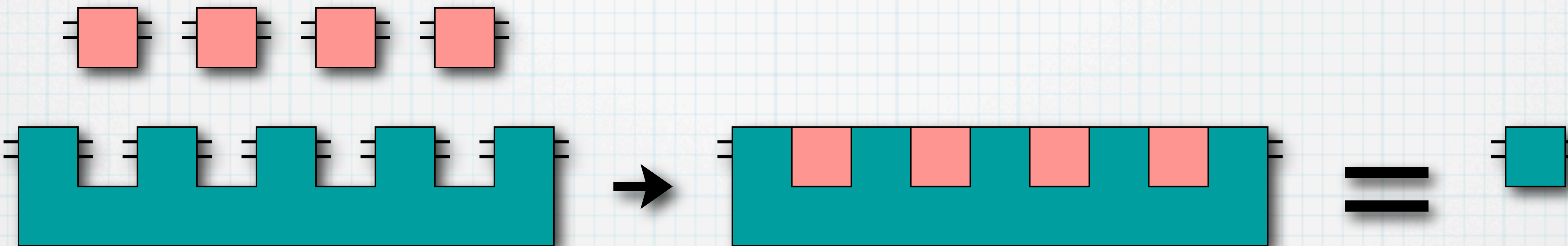
Causality constraints: (N+1 inputs/outputs)

$$\mathrm{Tr}_{2n-1}[R^{(n)}] = I_{2n-2} \otimes R^{(n-1)}, \quad n = 1, \ldots, N$$

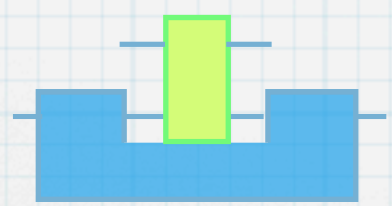
$$R^{(0)} = 1, \quad R^{(n)} = R$$

Supermaps

A quantum comb performs a transformation that is a generalization of the quantum operation: the so called "supermap"

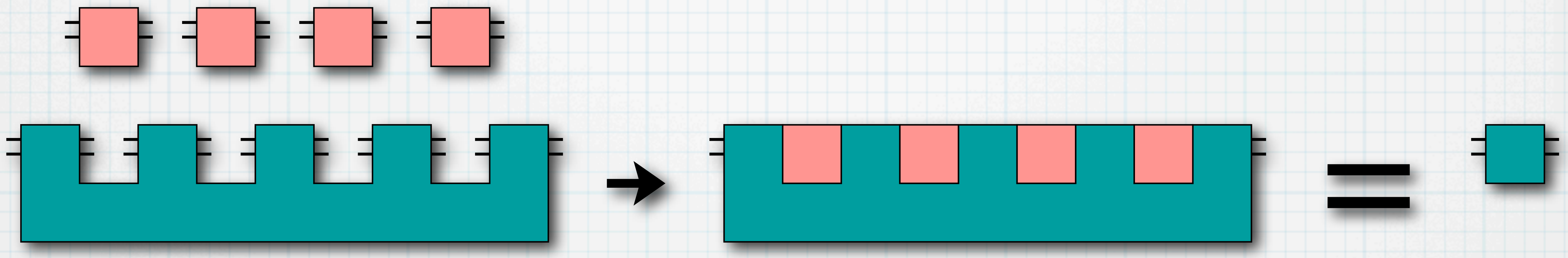


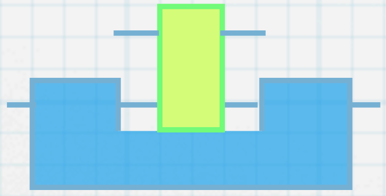
A supermap sends a series of N channels to one channel, also when applied locally, e.g.



Supermaps

A quantum comb performs a transformation that is a generalization of the quantum operation: the so called "supermap"

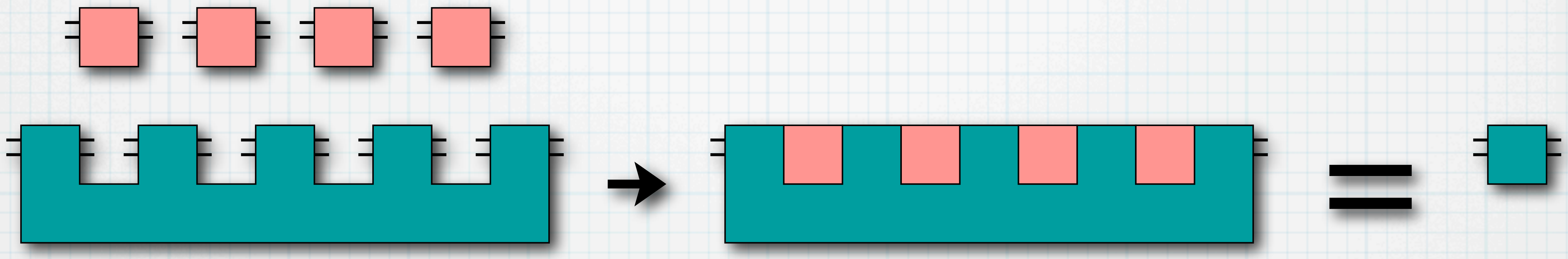


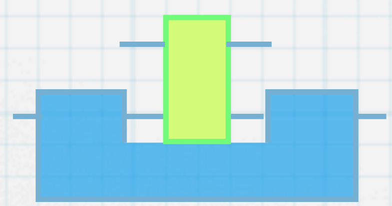
A supermap sends a series of N channels to one channel, also when applied locally, e.g. 

Mathematically it is represented by a CP N-linear map which sends N Choi operators to one Choi operator, and with his own Choi operator satisfying the causality constraints.

Supermaps

A quantum comb performs a transformation that is a generalization of the quantum operation: the so called "supermap"



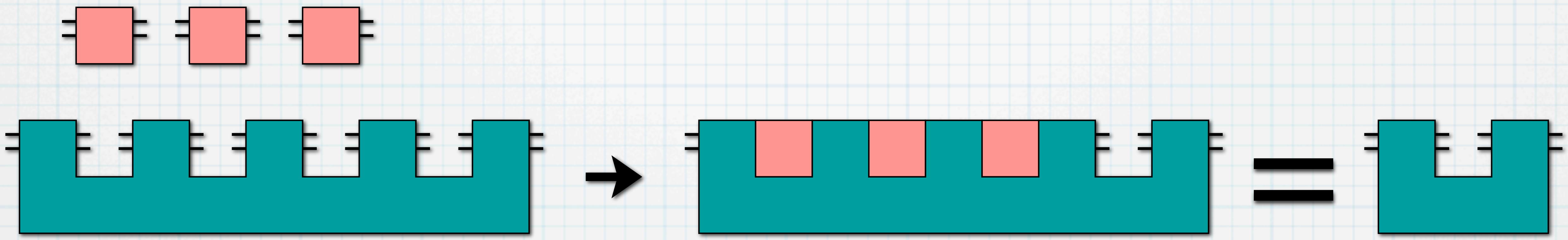
A supermap sends a series of N channels to one channel, also when applied locally, e.g. 

Mathematically it is represented by a CP N-linear map which sends N Choi operators to one Choi operator, and with his own Choi operator satisfying the causality constraints.

(we can likewise consider probabilistic supermaps).

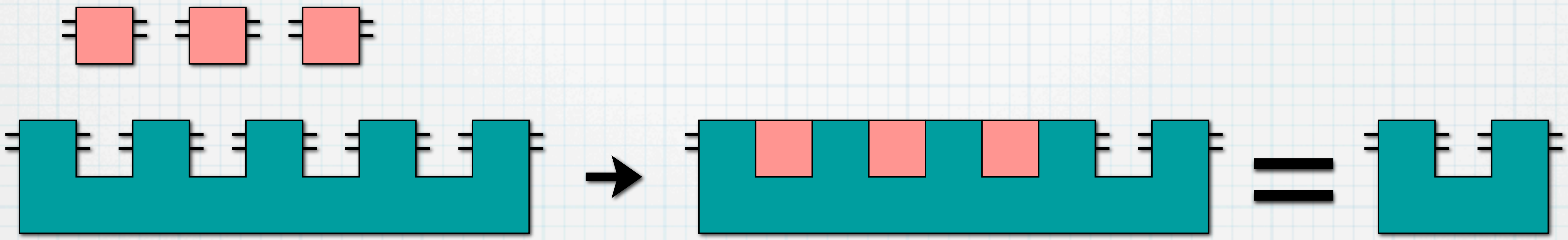
Supermaps

More generally, a quantum comb maps a series of channels into a comb

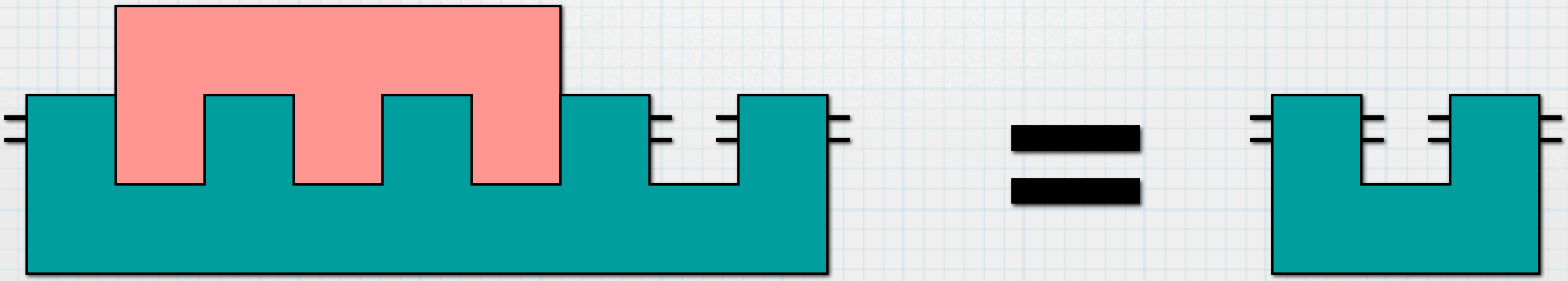


Supermaps

More generally, a quantum comb maps a series of channels into a comb



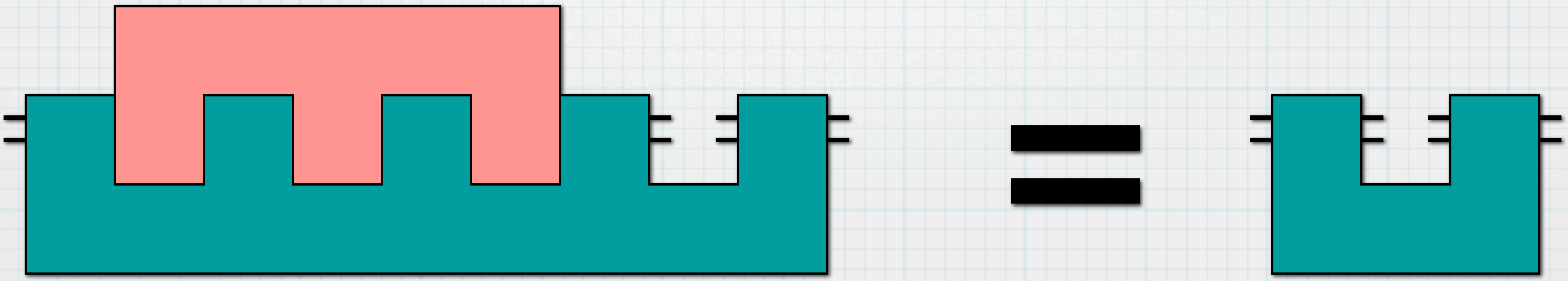
or, even more generally, a comb to a comb



PRL 101 060401 (2008)

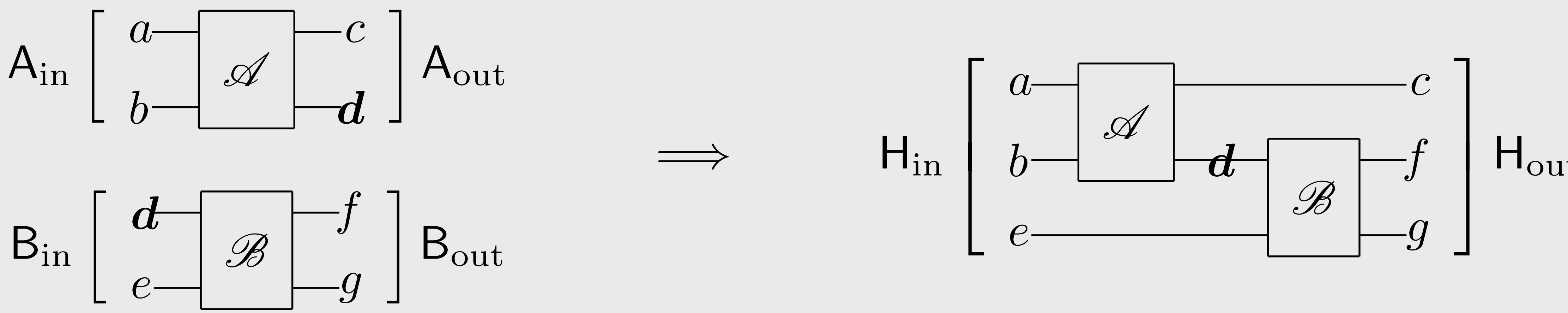
Supermaps

The notion of supermap is the last level of generalization, i.e. “super-supermaps” (mapping supermaps to supermaps) are still supermaps = quantum combs.



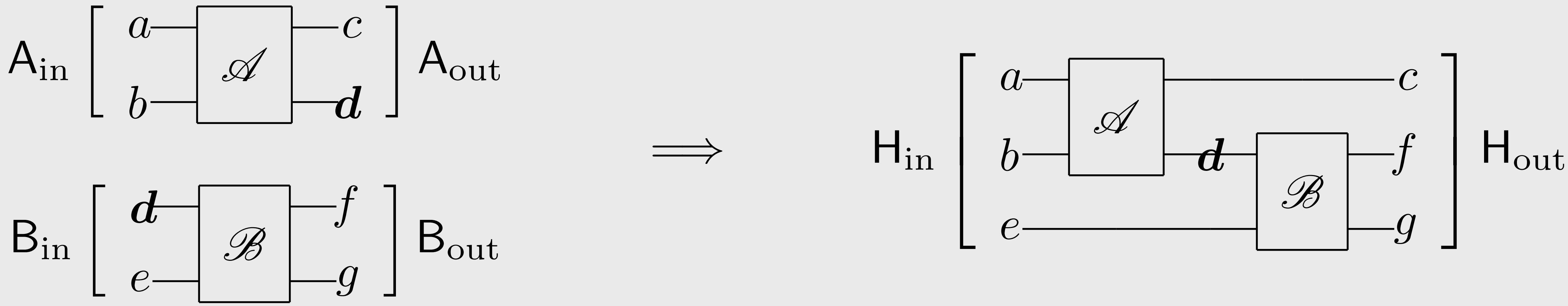
Link product

PRL 101 060401 (2008)



Link product

PRL 101 060401 (2008)



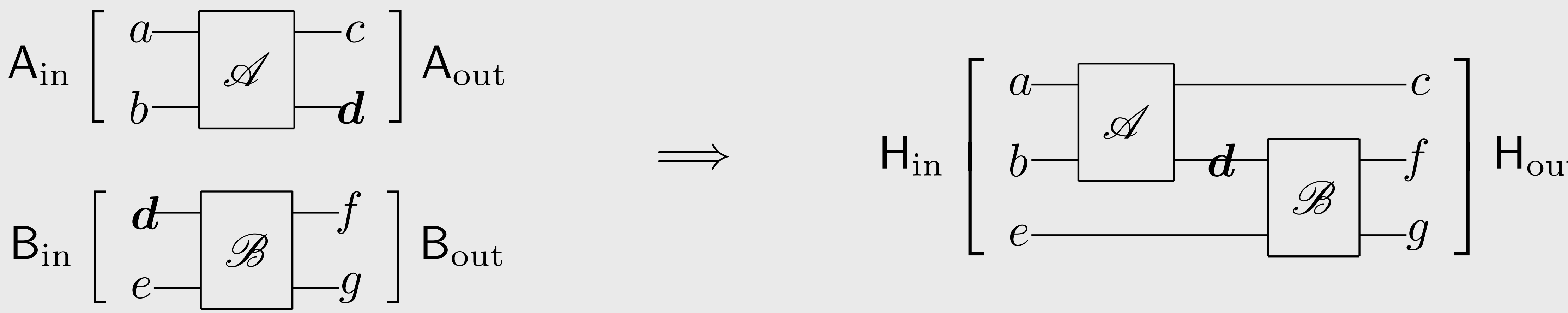
Choi-operator calculus

$$A \in \mathsf{B}(\mathsf{A}_{\mathrm{out}} \otimes \mathsf{A}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_a \otimes \mathsf{H}_b \otimes \mathsf{H}_c \otimes \mathsf{H}_{\boldsymbol{d}}), \qquad \mathsf{J} \equiv \mathsf{H}_{\boldsymbol{d}}$$

$$B \in \mathsf{B}(\mathsf{B}_{\mathrm{out}} \otimes \mathsf{B}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_{\boldsymbol{d}} \otimes \mathsf{H}_e \otimes \mathsf{H}_f \otimes \mathsf{H}_g)$$

PRL 101 060401 (2008)

Link product



Choi-operator calculus

$$A \in \mathsf{B}(\mathsf{A}_{\mathrm{out}} \otimes \mathsf{A}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_a \otimes \mathsf{H}_b \otimes \mathsf{H}_c \otimes \mathsf{H}_{\boldsymbol{d}}), \qquad \mathsf{J} \equiv \mathsf{H}_{\boldsymbol{d}}$$

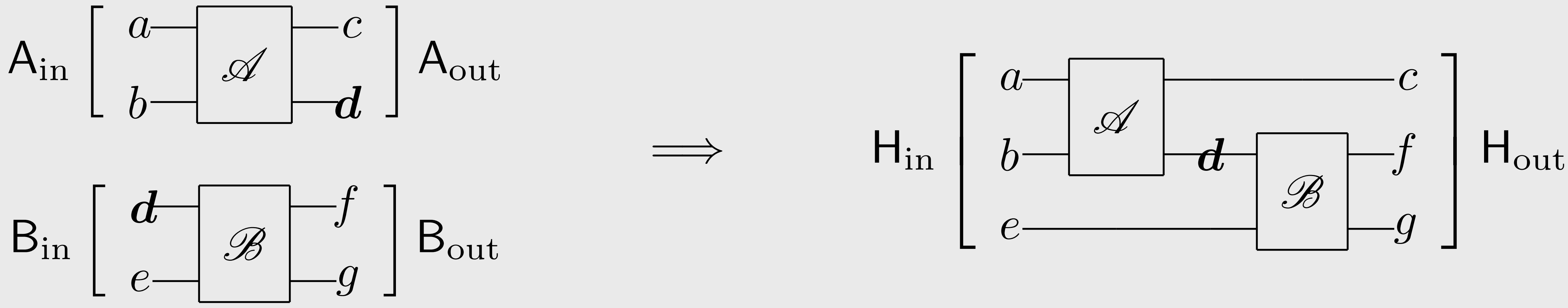
$$B \in \mathsf{B}(\mathsf{B}_{\mathrm{out}} \otimes \mathsf{B}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_{\boldsymbol{d}} \otimes \mathsf{H}_e \otimes \mathsf{H}_f \otimes \mathsf{H}_g)$$

$$AB := (A \otimes I_{e,f,g})(I_{a,b,c} \otimes B)$$

quantum information theory group

PRL 101 060401 (2008)

Link product



Choi-operator calculus

$$A \in \mathsf{B}(\mathsf{A}_{\mathrm{out}} \otimes \mathsf{A}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_a \otimes \mathsf{H}_b \otimes \mathsf{H}_c \otimes \mathsf{H}_{\boldsymbol{d}}), \qquad \mathsf{J} \equiv \mathsf{H}_{\boldsymbol{d}}$$

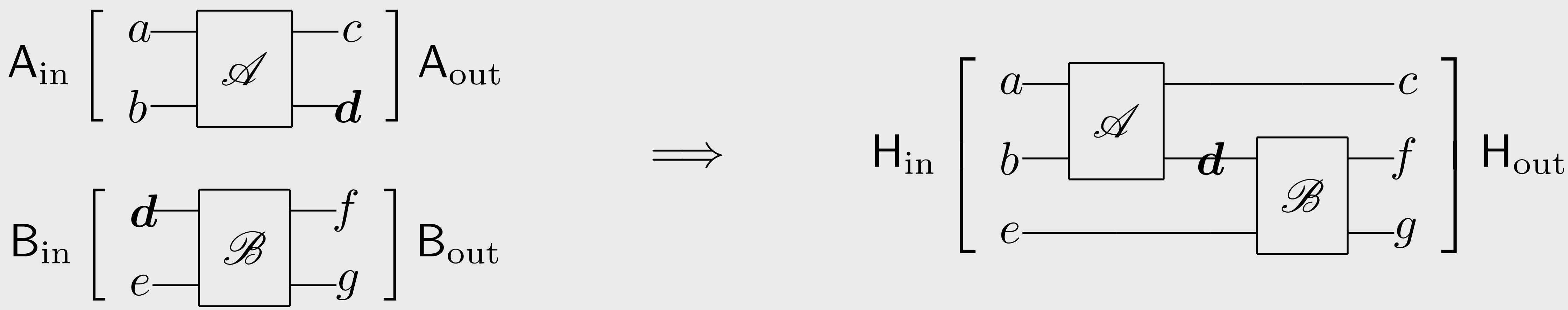
$$B \in \mathsf{B}(\mathsf{B}_{\mathrm{out}} \otimes \mathsf{B}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_{\boldsymbol{d}} \otimes \mathsf{H}_e \otimes \mathsf{H}_f \otimes \mathsf{H}_g)$$

$$AB := (A \otimes I_{e,f,g})(I_{a,b,c} \otimes B)$$

$$\boxed{A * B = \mathrm{Tr}_{\mathsf{J}}[A^{\theta_{\mathsf{J}}} B] \in \mathsf{B}(\mathsf{H}_{\mathrm{out}} \otimes \mathsf{H}_{\mathrm{in}})}$$

PRL 101 060401 (2008)

Link product



Choi-operator calculus

$$A \in \mathsf{B}(\mathsf{A}_{\mathrm{out}} \otimes \mathsf{A}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_a \otimes \mathsf{H}_b \otimes \mathsf{H}_c \otimes \mathsf{H}_{\boldsymbol{d}}), \qquad \mathsf{J} \equiv \mathsf{H}_{\boldsymbol{d}}$$

$$B \in \mathsf{B}(\mathsf{B}_{\mathrm{out}} \otimes \mathsf{B}_{\mathrm{in}}) = \mathsf{B}(\mathsf{H}_{\boldsymbol{d}} \otimes \mathsf{H}_e \otimes \mathsf{H}_f \otimes \mathsf{H}_g)$$

$$AB := (A \otimes I_{e,f,g})(I_{a,b,c} \otimes B)$$

$$\boxed{A * B = \mathrm{Tr}_{\mathsf{J}}[A^{\theta_{\mathsf{J}}} B] \in \mathsf{B}(\mathsf{H}_{\mathrm{out}} \otimes \mathsf{H}_{\mathrm{in}})}$$

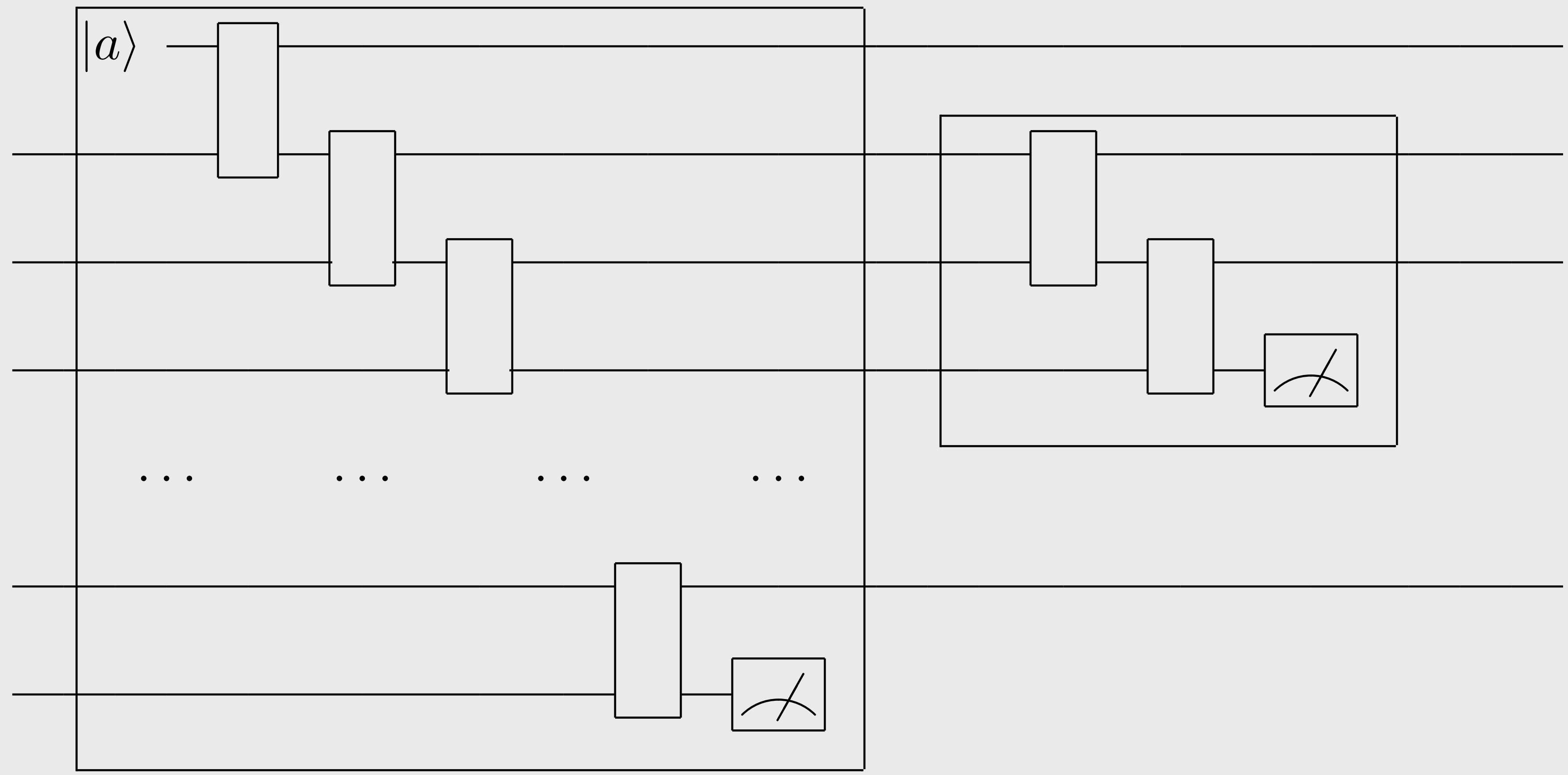
The link-product is commutative!

QUit quantum information theory group

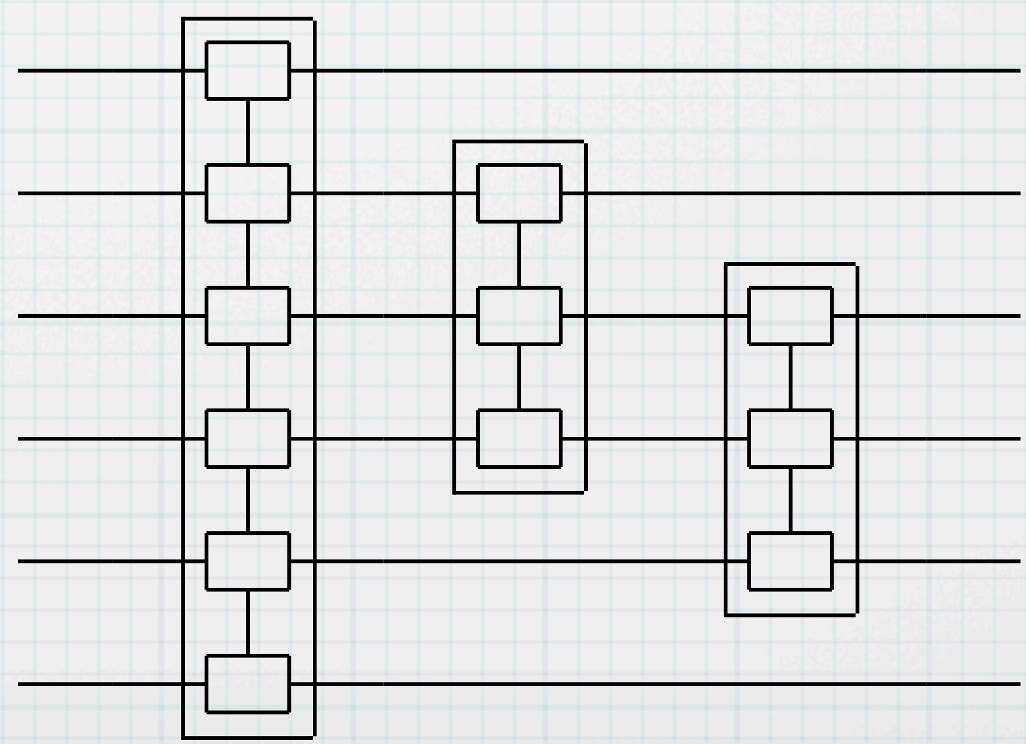
PRL 101 060401 (2008)

Link product

$R_1 * R_2 \qquad \Longleftrightarrow$



$$R_1 * R_2 * R_3 \qquad \Longleftrightarrow$$



PRL 101 060401 (2008)

Link product

Special cases:

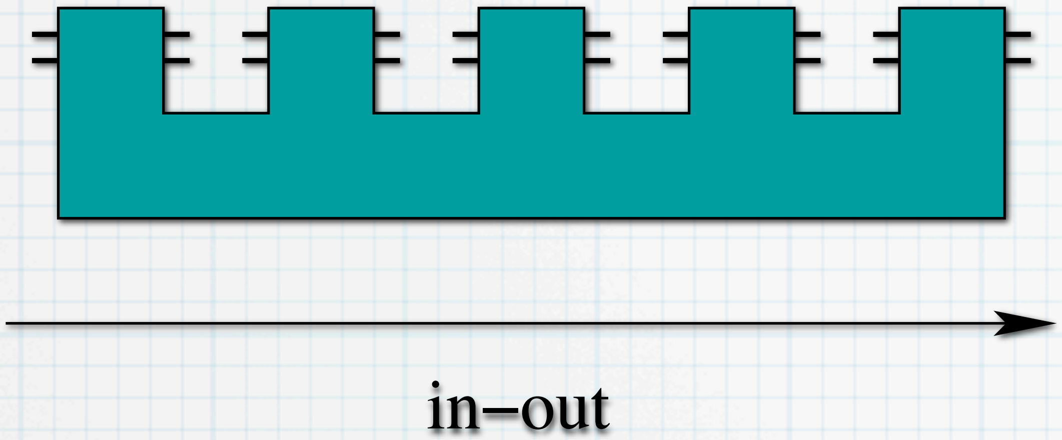
$$\mathscr{M}(\rho) = R_{\mathscr{M}} * \rho$$ quantum operation

$$\mathrm{Tr}[P^t \rho] = P * \rho$$ POVM

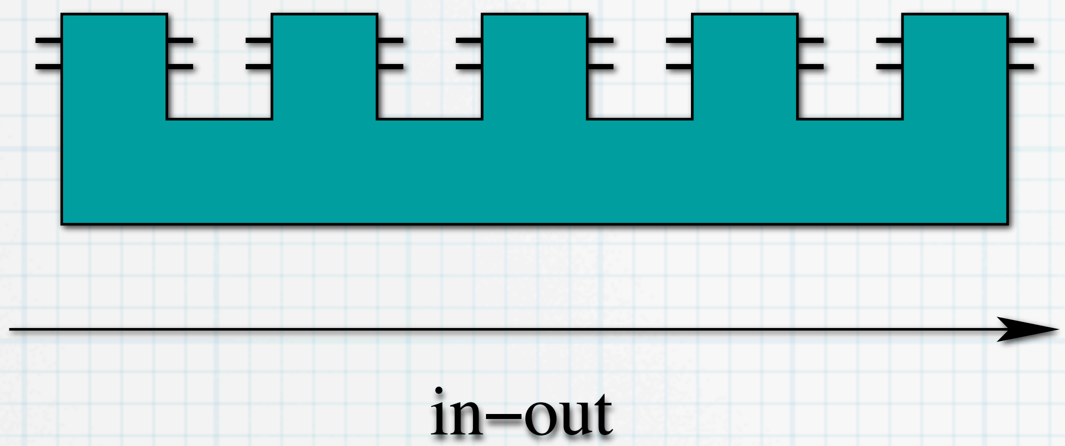
$$\rho \bigotimes \sigma = \rho * \sigma$$ tensor product

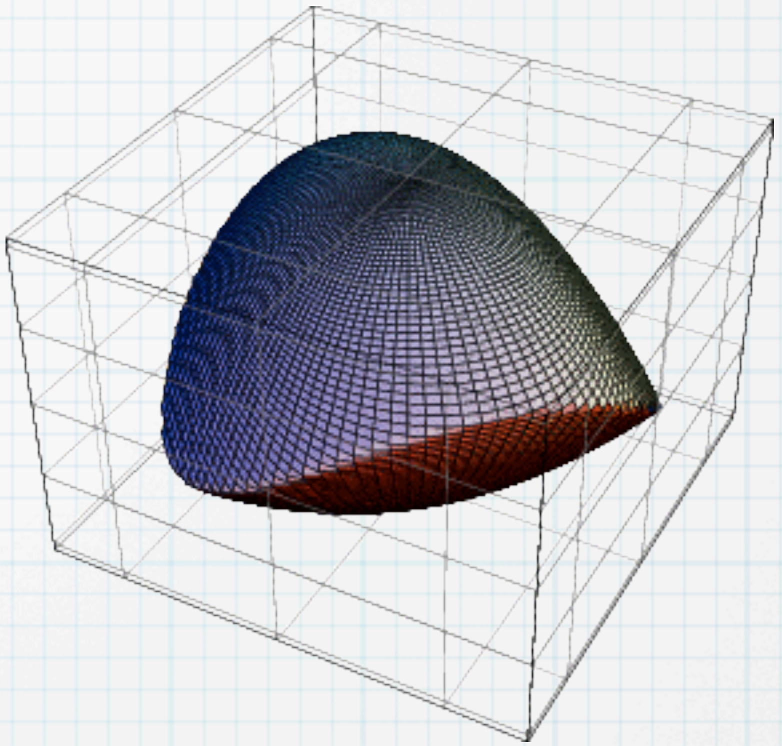
$$\mathrm{Tr}_{\mathsf{H}}[R] = R * I_{\mathsf{H}}$$ partial trace

Circuits Architecture Optimization



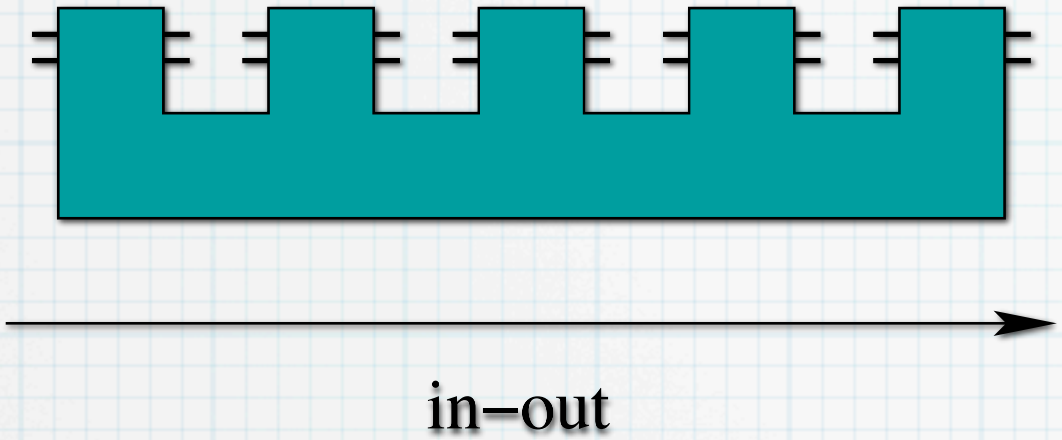
Circuits Architecture Optimization

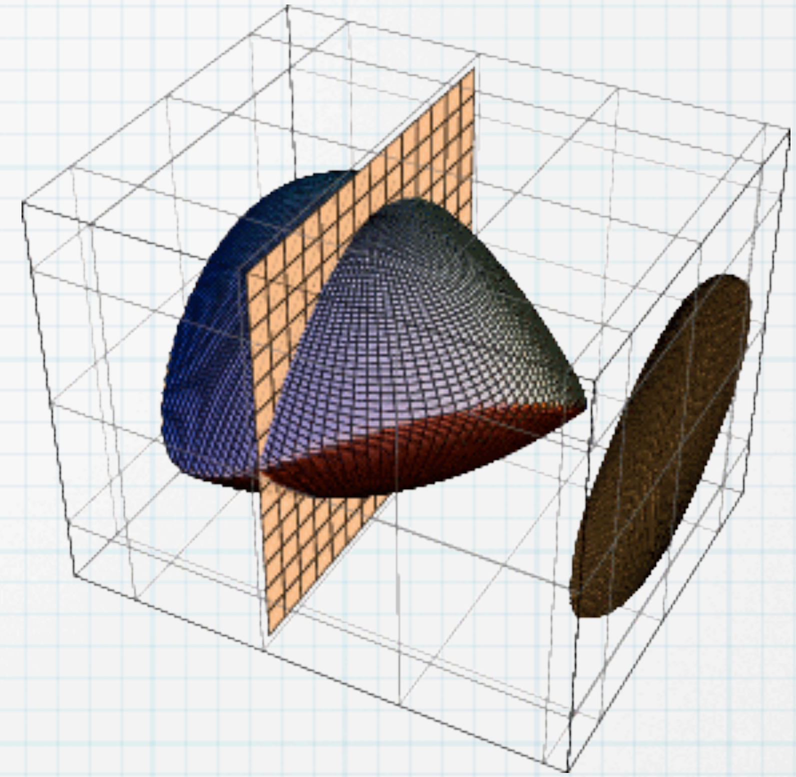




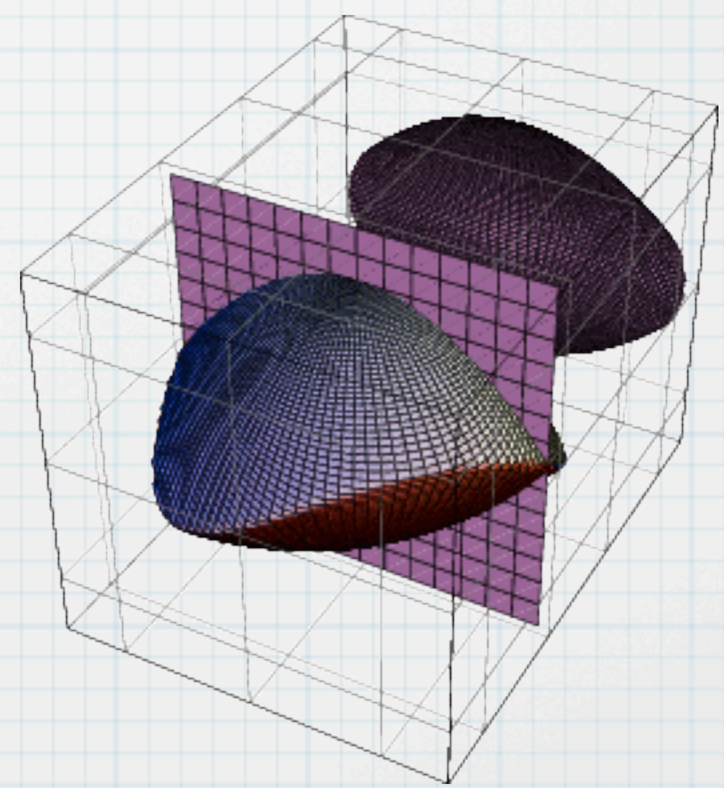
- The Choi operators of a fixed input-output comb structure make a convex set

Circuits Architecture Optimization





- The Choi operators of a fixed input-output comb structure make a convex set
- Causality constraints correspond to a hyperplane section of the convex
- Group-covariance gives another linear constraint:



$$[R, V_g] = 0 \implies R = \bigoplus_j R_j \otimes \mathbb{1}_{m_j}$$

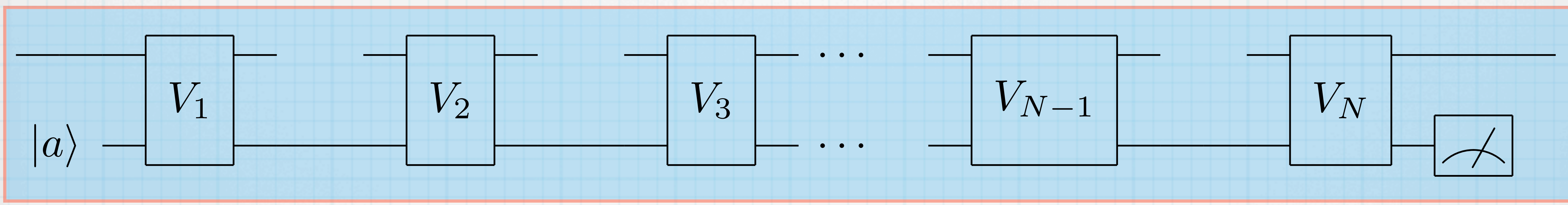
QUit quantum information theory group

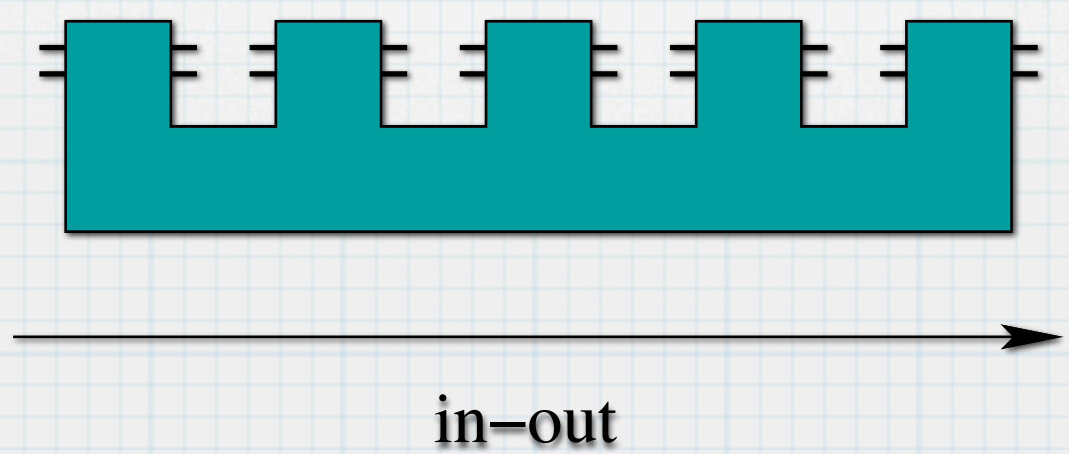
The mathematical formulation is reduced to a convex problem!

Realization theorem

Chiribella, D’Ariano, Perinotti, PRL **101** 060401 (2008) EL **83** 30004 (2008)

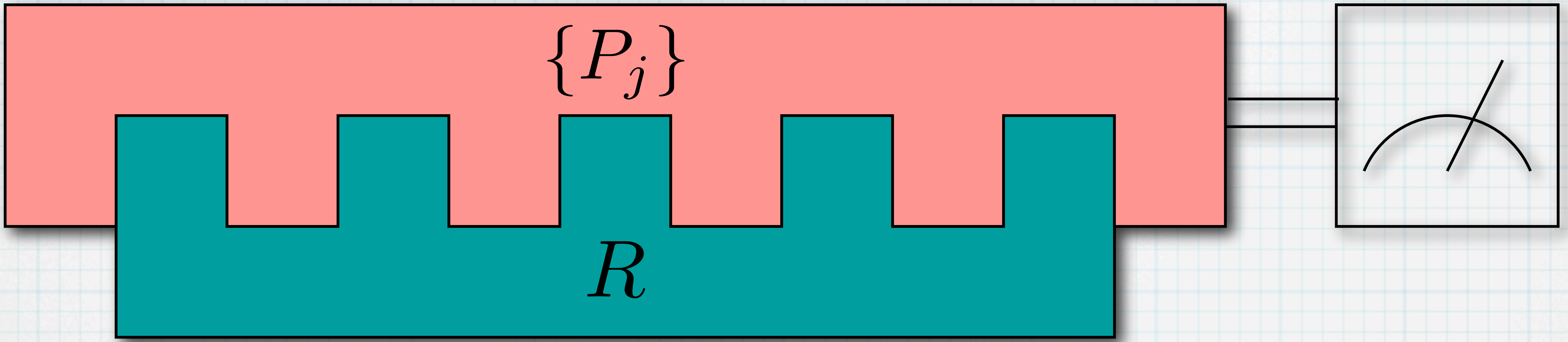
Theorem: Every Choi operator on given input-output spaces and satisfying given causality conditions is realized by the comb of isometries





For realization of isometries see: Buscemi, D'Ariano, and Sacchi, PRA 68 042113 (2003)

Quantum board testers



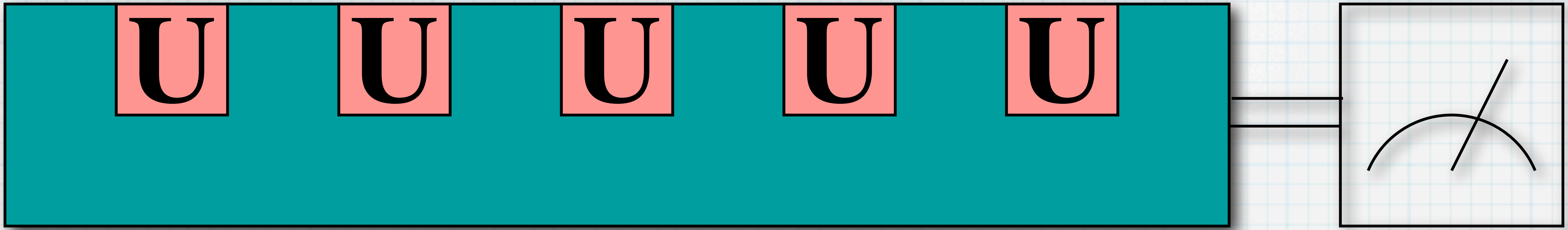
Tester
Born rule:

$$\mathrm{Tr}[P_j R] = p_j, \qquad \sum_j P_j = \Xi$$

causality constraints:

$$\mathrm{Tr}_{2n+1}[\Xi^{(n)}] = I_{2n} \otimes \Xi^{(n-1)}, \; n = 0, 1, \ldots, N$$
$$\Xi^{(N)} \equiv \Xi, \; \mathrm{Tr}_1[\Xi^{(0)}] = 1$$

Estimating tester



Tester

Born rule:

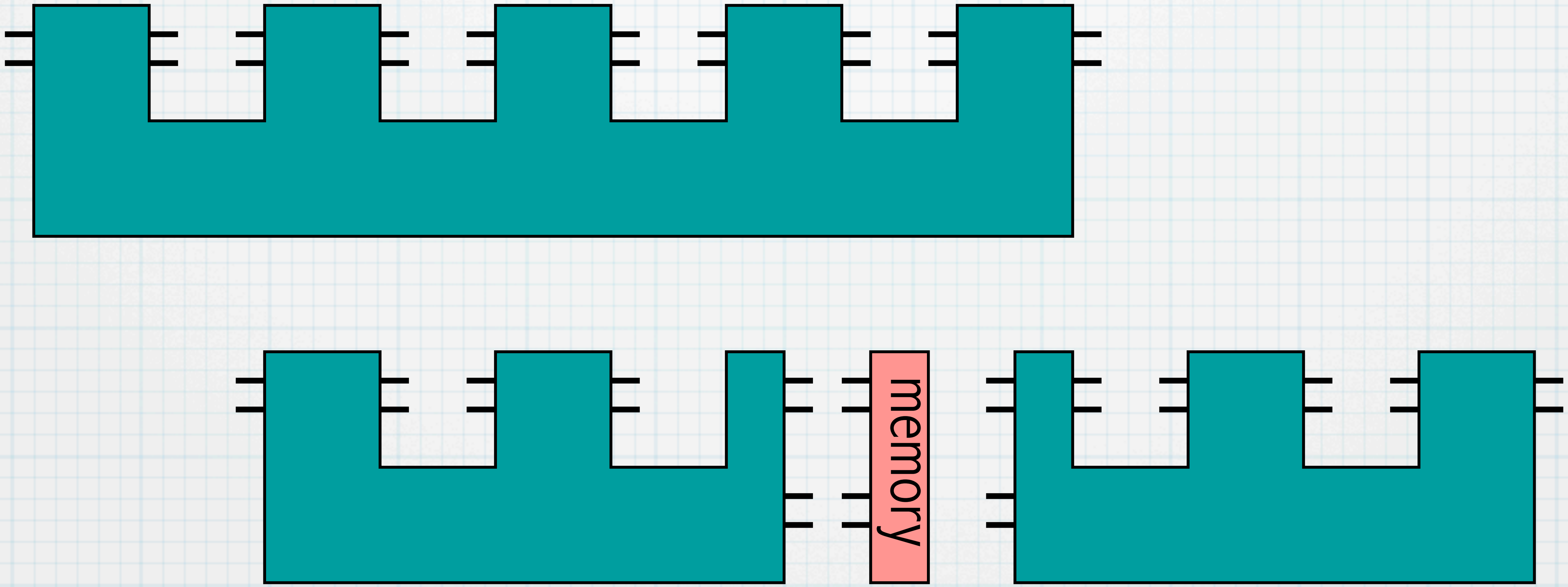
$$\mathrm{Tr}[P_j R] = p_j, \qquad \sum_j P_j = \Xi$$

causality constraints:

$$\mathrm{Tr}_{2n+1}[\Xi^{(n)}] = I_{2n} \otimes \Xi^{(n-1)}, \; n = 0, 1, \ldots, N$$
$$\Xi^{(N)} \equiv \Xi, \; \mathrm{Tr}_1[\Xi^{(0)}] = 1$$

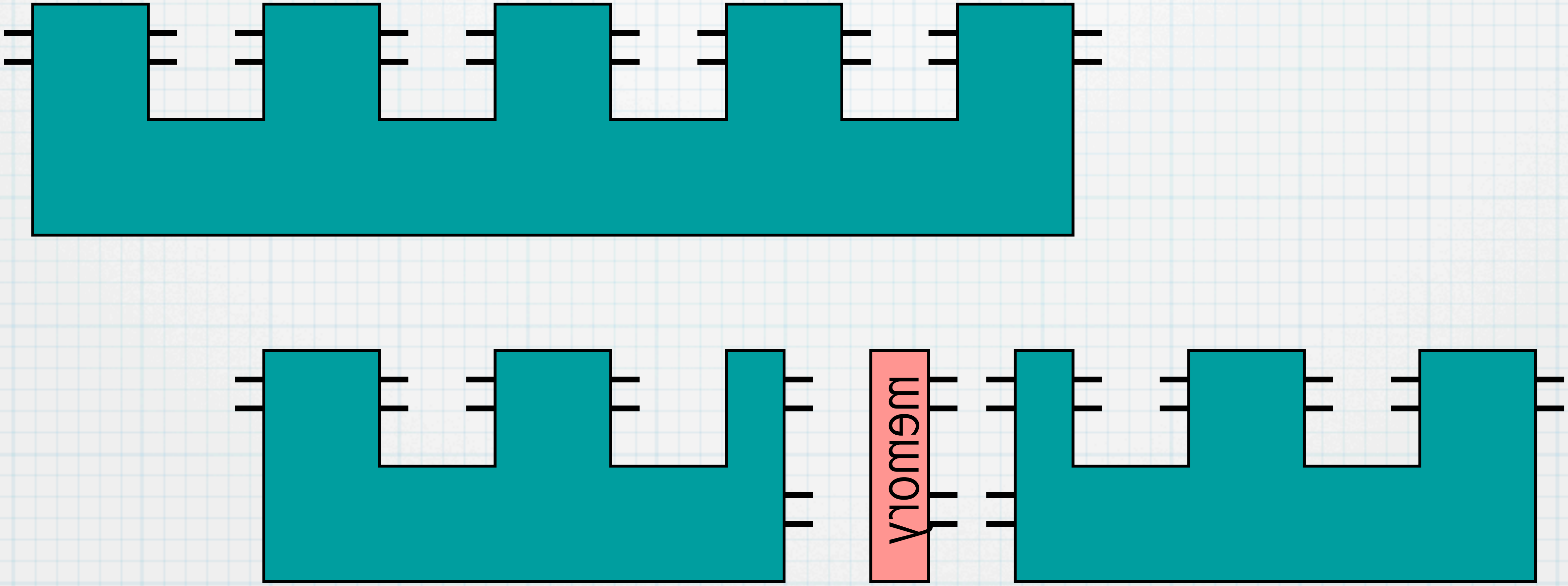
Using quantum memory

delay the use of subcircuits by breaking the comb into subcombs + quantum memory



Using quantum memory

delay the use of subcircuits by breaking the comb into subcombs + quantum memory



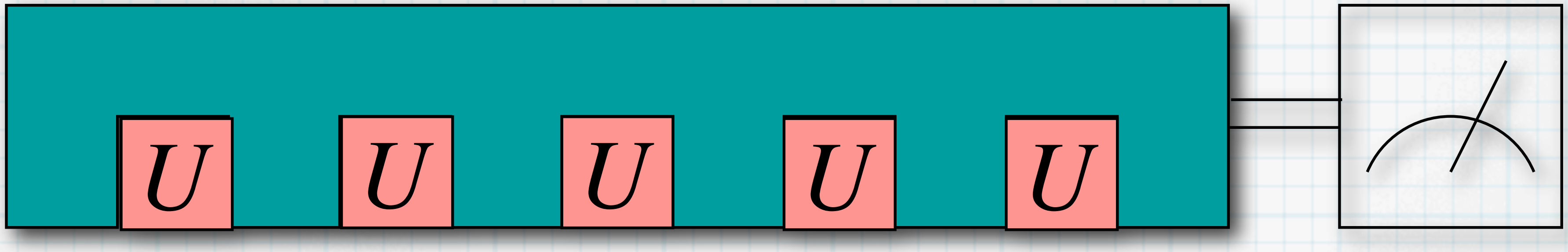
Applications

Application 1: discrimination and estimation of unitaries (optimal oracle-calling quantum algorithms)

Discrimination of unitaries

Chiribella, D'Ariano, Perinotti, PRL 101 180501 (2008)

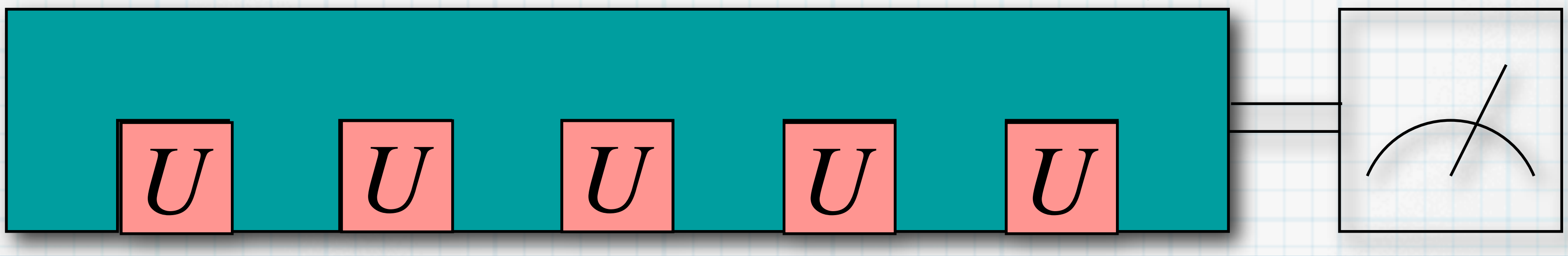
Optimal discrimination between two possible unitary operators U_1 U_2

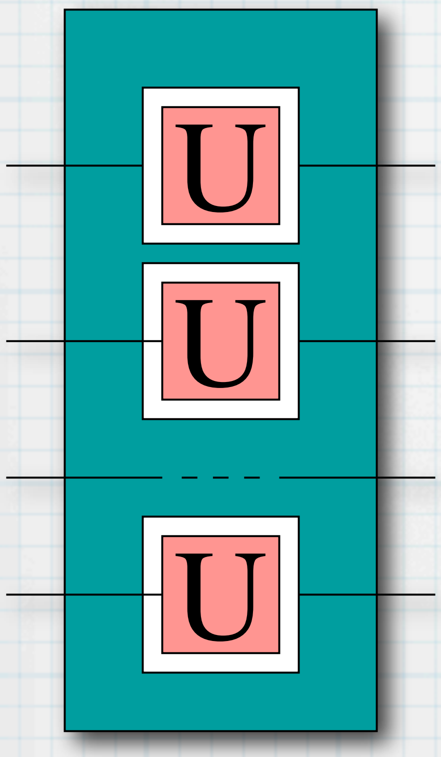


Discrimination of unitaries

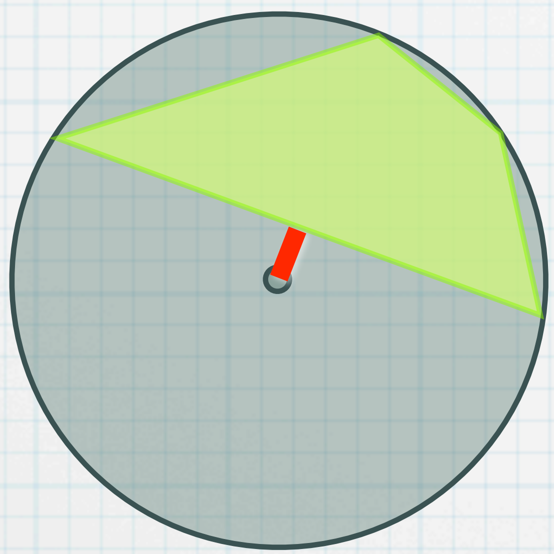
Chiribella, D'Ariano, Perinotti, PRL 101 180501 (2008)

Optimal discrimination between two possible unitary operators U_1 U_2





$$V = U_1^\dagger U_2$$



G. M. D'Ariano, P. Lo Presti, M. G. A. Paris, PRL 87, 270404 (2001); A. Acín, PRL 87, 177901(2001).

angular spread $\Delta(U)$

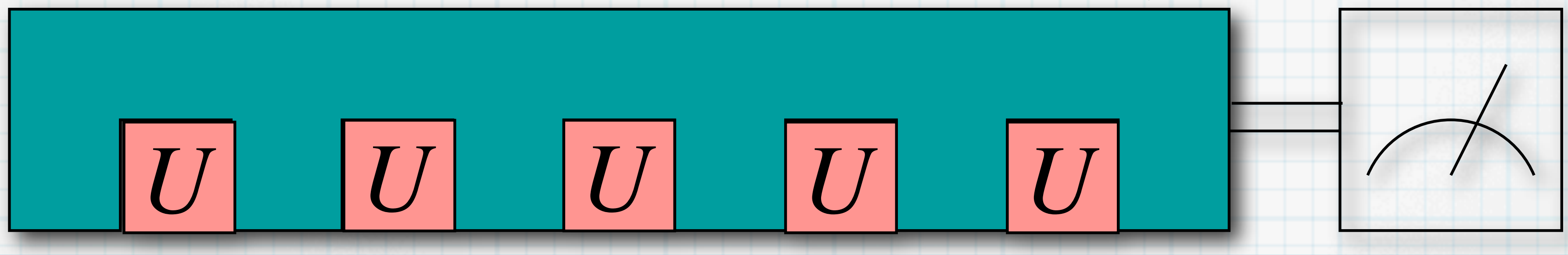
$$\Delta(U \otimes V) = \Delta(U) + \Delta(V)$$

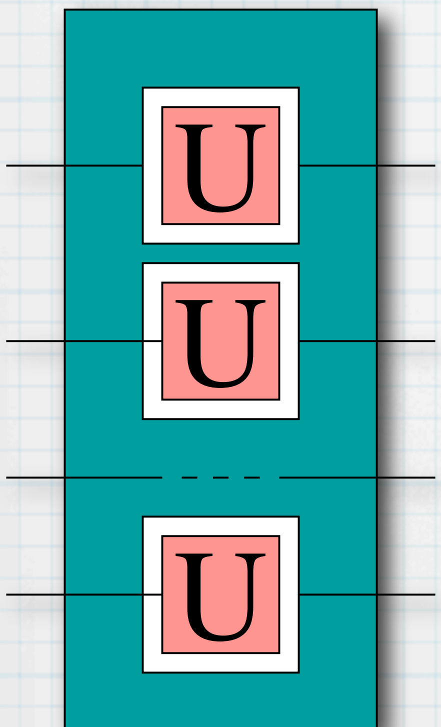
$$N = \left\lceil \frac{\pi}{\Delta\phi} \right\rceil$$

Discrimination of unitaries

Chiribella, D'Ariano, Perinotti, PRL 101 180501 (2008)

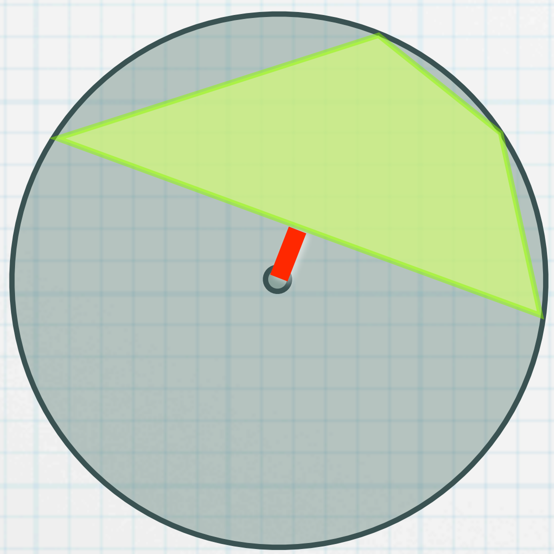
Optimal discrimination between two possible unitary operators U_1 U_2





$$V = U_1^\dagger U_2$$

G. M. D'Ariano, P. Lo Presti, M. G. A. Paris, PRL 87, 270404 (2001); A. Acín, PRL 87, 177901(2001).



angular spread $\Delta(U)$

$$\Delta(U \otimes V) = \Delta(U) + \Delta(V)$$

$$N = \left\lceil \frac{\pi}{\Delta\phi} \right\rceil$$

spread lemma: $\Delta(AB) \leq \Delta(A) + \Delta(B)$ A M Childs, J Preskill, and J Renes, JMO 47, 155-176 (2000).

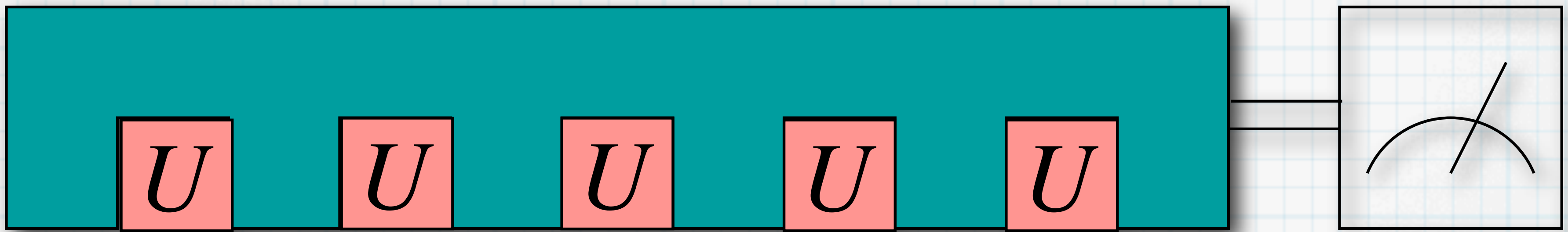
$$\Delta[W(U \otimes I)W^\dagger(U \otimes I)] \leq \Delta(U^{\otimes 2})$$

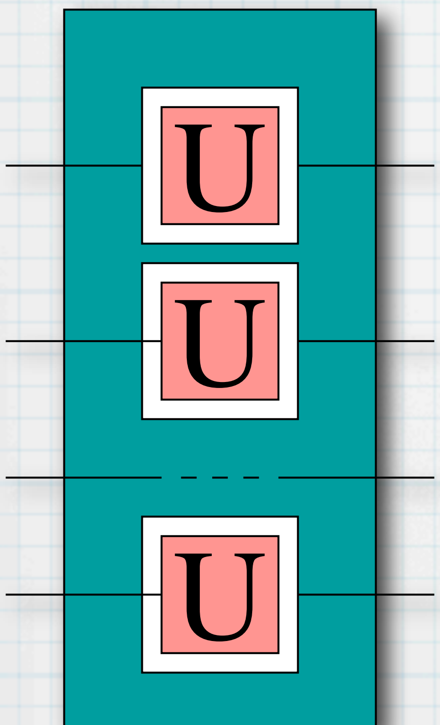
The spread of the tester is not larger than that of $U^{\otimes N}$ and U^N

Discrimination of unitaries

Chiribella, D'Ariano, Perinotti, PRL 101 180501 (2008)

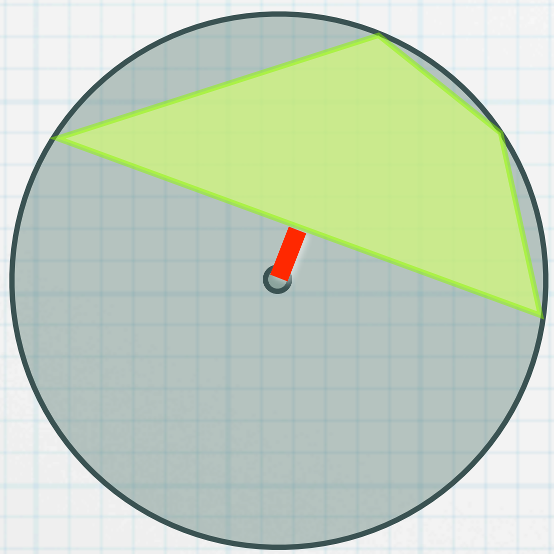
Optimal discrimination between two possible unitary operators U_1 U_2





$$V = U_1^\dagger U_2$$

G. M. D'Ariano, P. Lo Presti, M. G. A. Paris, PRL 87, 270404 (2001); A. Acín, PRL 87, 177901(2001).



angular spread $\Delta(U)$

$$\Delta(U \otimes V) = \Delta(U) + \Delta(V)$$

$$N = \left\lceil \frac{\pi}{\Delta\phi} \right\rceil$$

spread lemma: $\Delta(AB) \leq \Delta(A) + \Delta(B)$ A M Childs, J Preskill, and J Renes, JMO 47, 155-176 (2000).

$$\Delta[W(U \otimes I)W^\dagger(U \otimes I)] \leq \Delta(U^{\otimes 2})$$

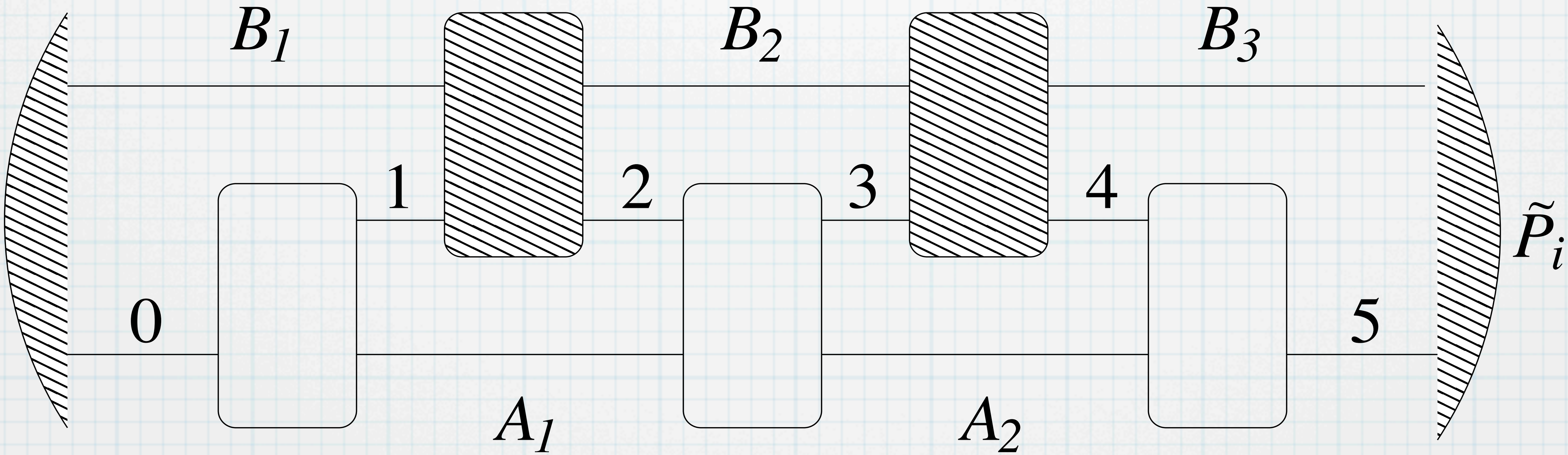
The spread of the tester is not larger than that of $U^{\otimes N}$and U^N

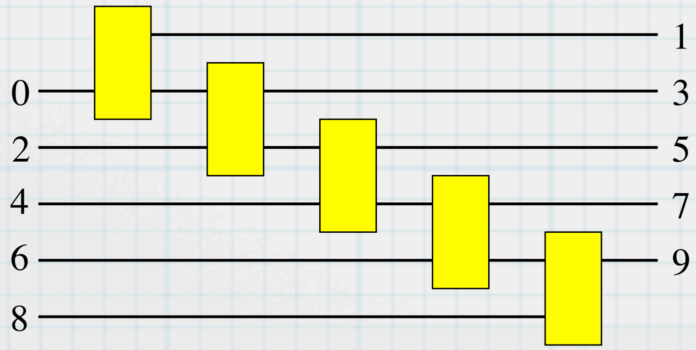
The parallel diposition is already optimal

Discrimination of memory channels

PRL **101** 180501 (2008)

There are memory channels that can be discriminated perfectly with a single use by a quantum tester, and not conventionally



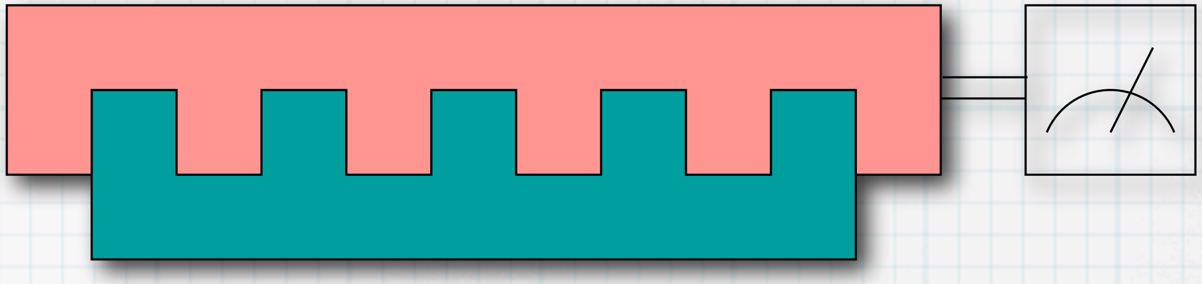


Discrimination of memory channels

Chiribella, D'Ariano, Perinotti, (unpublished)

Tester Born rule:

$$\mathrm{Tr}[P_j R] = p_j, \qquad \sum_j P_j = \Xi$$



Perfect discrimination for:

$$R_1(I \otimes \Xi)R_2 = 0$$

Discrimination of unitaries

- What happens for more than two unitaries?
- What happens for non-unitary channels?

Covariant estimation of unitaries

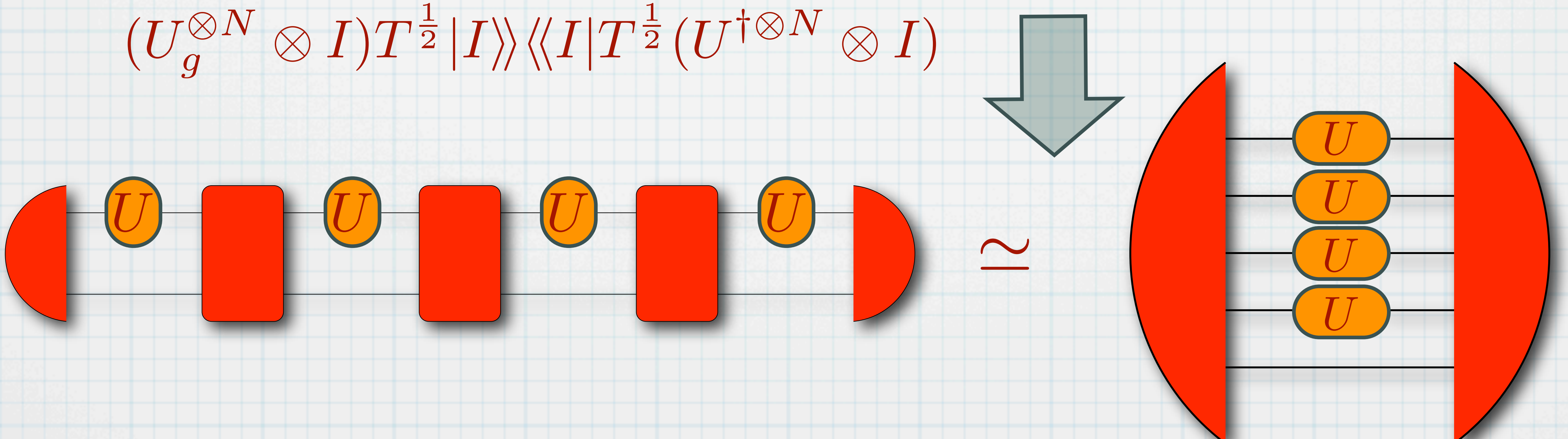
- Covariant unitary estimation problem (group of unitaries, Haar-distributed)
- Problem: find the optimal tester for estimating the group element

One can prove that the optimal tester is covariant:

$$T = \int_G \mathrm{d}\, g T_g \qquad T_h = (U_h^{\otimes N} \otimes I)\Theta(U_h^{\dagger\otimes N} \otimes I) \quad \Rightarrow \quad [T, U_h^{\otimes N} \otimes I] = 0$$

Then: $T^{\frac{1}{2}}(|U_g\rangle\!\rangle\langle\!\langle U_g|)^{\otimes N} T^{\frac{1}{2}} = T^{\frac{1}{2}}(U_g^{\otimes N} \otimes I)|I\rangle\!\rangle\langle\!\langle I|(U^{\dagger\otimes N} \otimes I)T^{\frac{1}{2}} =$

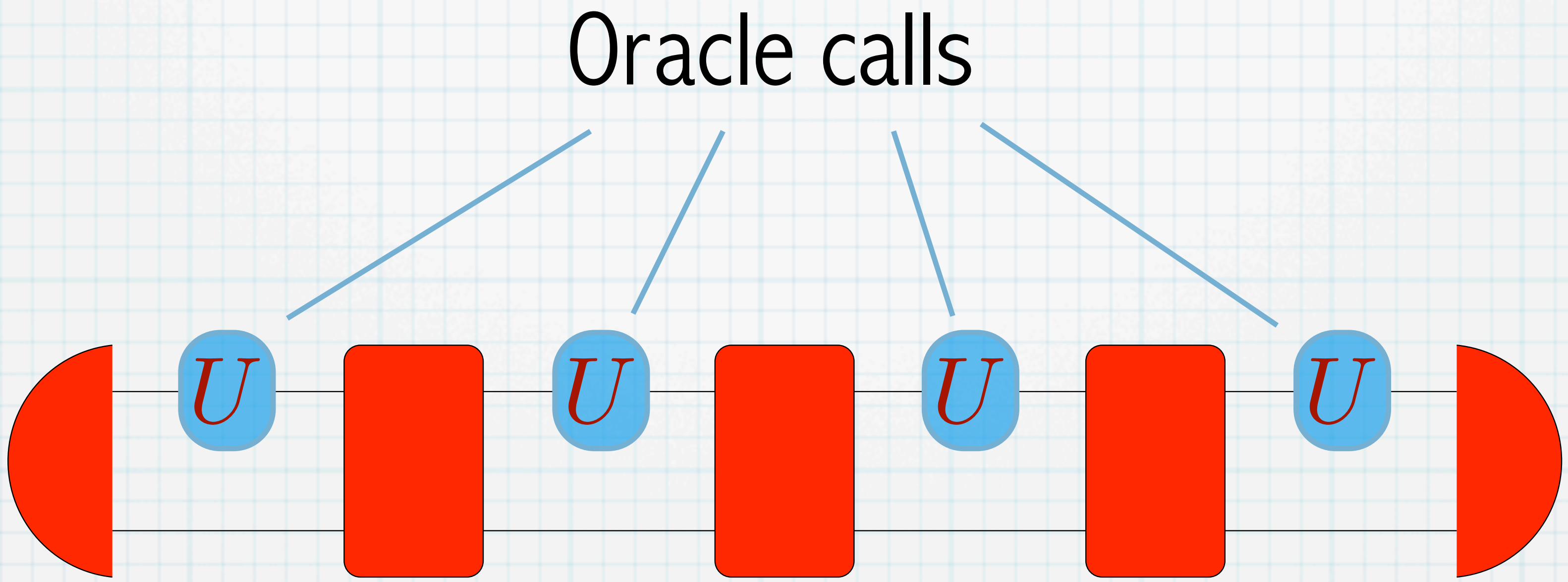
$$(U_g^{\otimes N} \otimes I)T^{\frac{1}{2}}|I\rangle\!\rangle\langle\!\langle I|T^{\frac{1}{2}}(U^{\dagger\otimes N} \otimes I)$$



Any covariant tester is equivalent to a parallel scheme

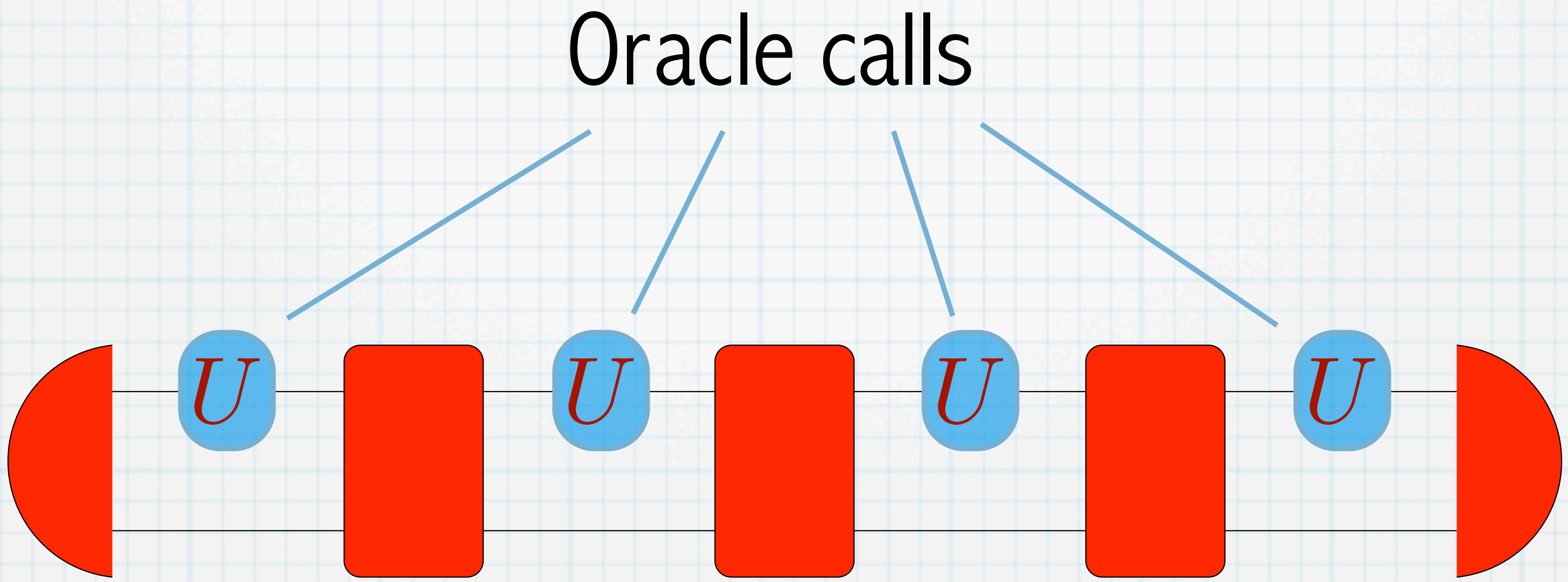
Discrimination of unitaries

Oracle-calling quantum algorithm as optimal discrimination of unitaries



Discrimination of unitaries

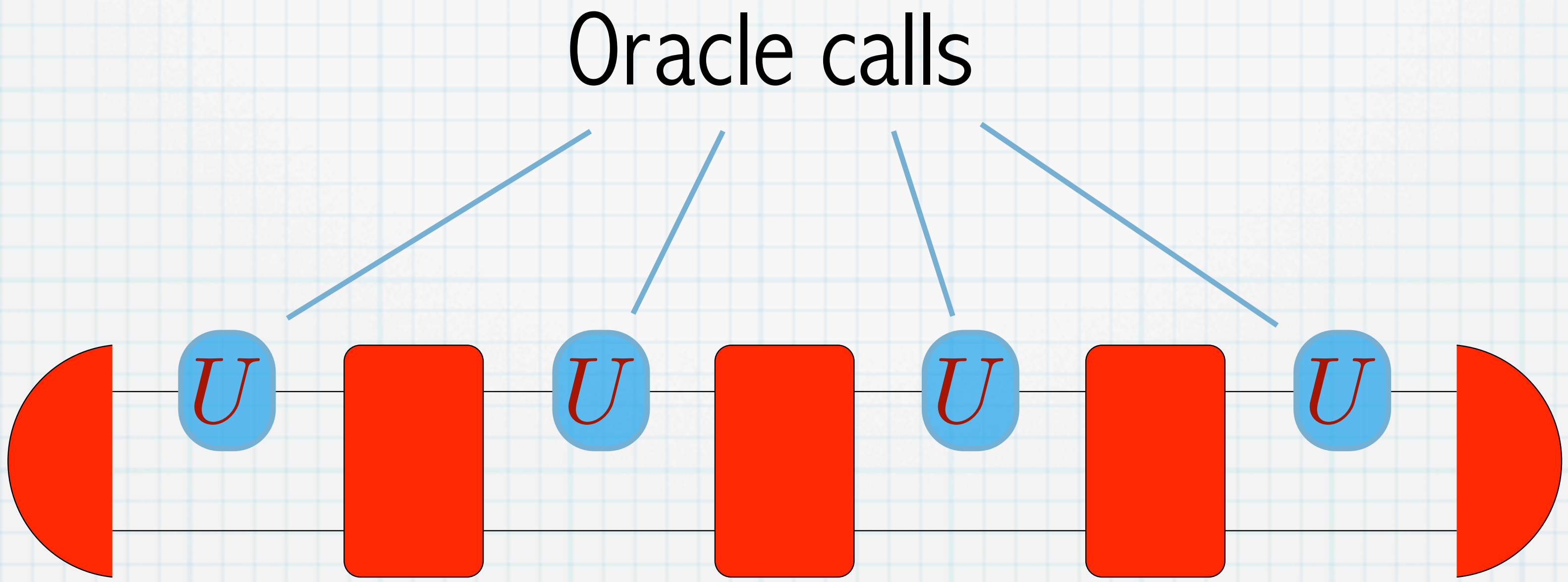
Oracle-calling quantum algorithm as optimal discrimination of unitaries



Hidden-subgroup algorithms (Deutsh-Jozsa, Simon, etc): parallel calls are optimal

Discrimination of unitaries

Oracle-calling quantum algorithm as optimal discrimination of unitaries

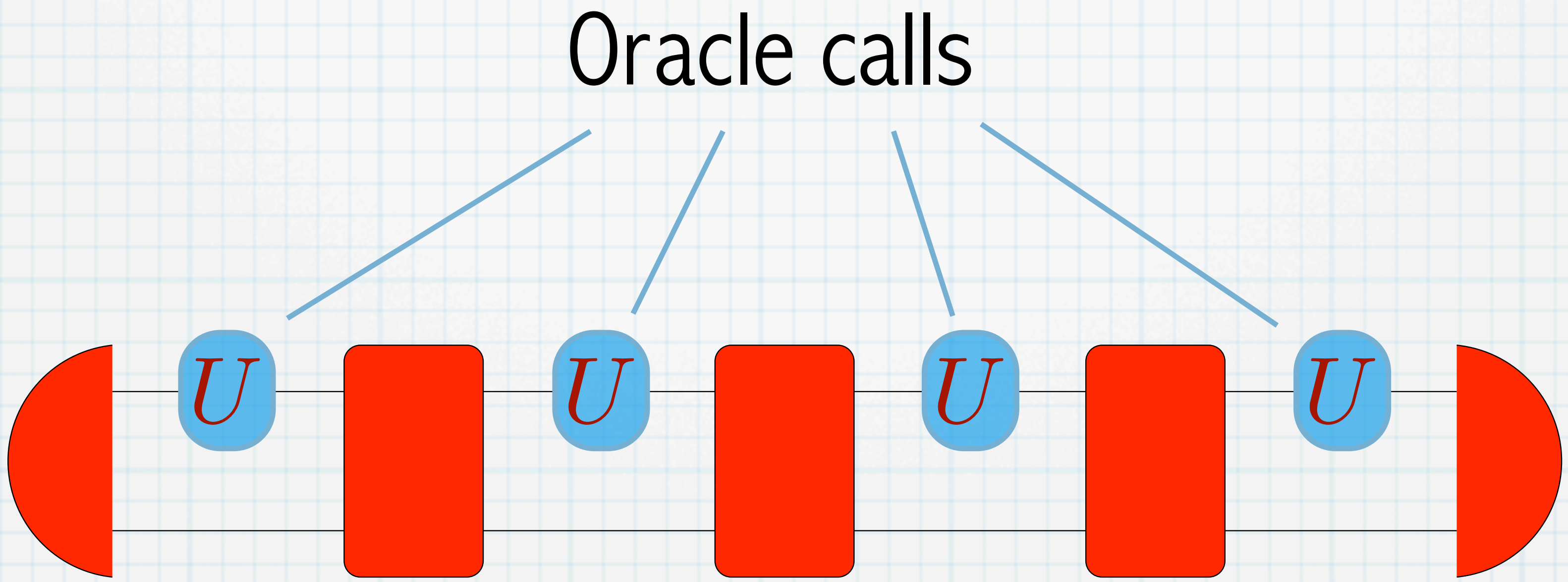


Hidden-subgroup algorithms (Deutsh-Jozsa, Simon, etc): parallel calls are optimal

Algorithms with no hidden subgroup (e.g. Grover) need a comb [C. Zalka, PRA 60, 2746 (1999)]

Discrimination of unitaries

Oracle-calling quantum algorithm as optimal discrimination of unitaries



Hidden-subgroup algorithms (Deutsh-Jozsa, Simon, etc): parallel calls are optimal

Algorithms with no hidden subgroup (e.g. Grover) need a comb [C. Zalka, PRA 60, 2746 (1999)]

Q-combs: systematic method to determine optimal oracle-calling algorithms

Discrimination of unitaries

When do we need a tester (not just a parallel discrimination):

Discrimination of unitaries

When do we need a tester (not just a parallel discrimination):

- For discrimination of non-unitary channels
- For discrimination within non-covariant sets
- For discrimination of memory channels

Operational network distance

PRL **101** 180501 (2008)

Existence of optimal non parallel optimal discrimination schemes

Operational network distance

PRL **101** 180501 (2008)

Existence of optimal non parallel optimal discrimination schemes

The proper distance for memory channels must be defined in terms of optimal discriminating testers

$$D(\mathscr{C}^{(N)}, \mathscr{D}^{(N)}) := \max_{\Xi^{(N)}} \left\| \left(I \otimes \Xi^{(N)\frac{1}{2}} \right) \Delta \left(I \otimes \Xi^{(N)\frac{1}{2}} \right) \right\|_1$$

$$\Delta := C - D$$

Operational network distance

PRL **101** 180501 (2008)

Existence of optimal non parallel optimal discrimination schemes

The proper distance for memory channels must be defined in terms of optimal discriminating testers

$$D(\mathscr{C}^{(N)}, \mathscr{D}^{(N)}) := \max_{\Xi^{(N)}} \left\| \left(I \otimes \Xi^{(N)\frac{1}{2}} \right) \Delta \left(I \otimes \Xi^{(N)\frac{1}{2}} \right) \right\|_1$$

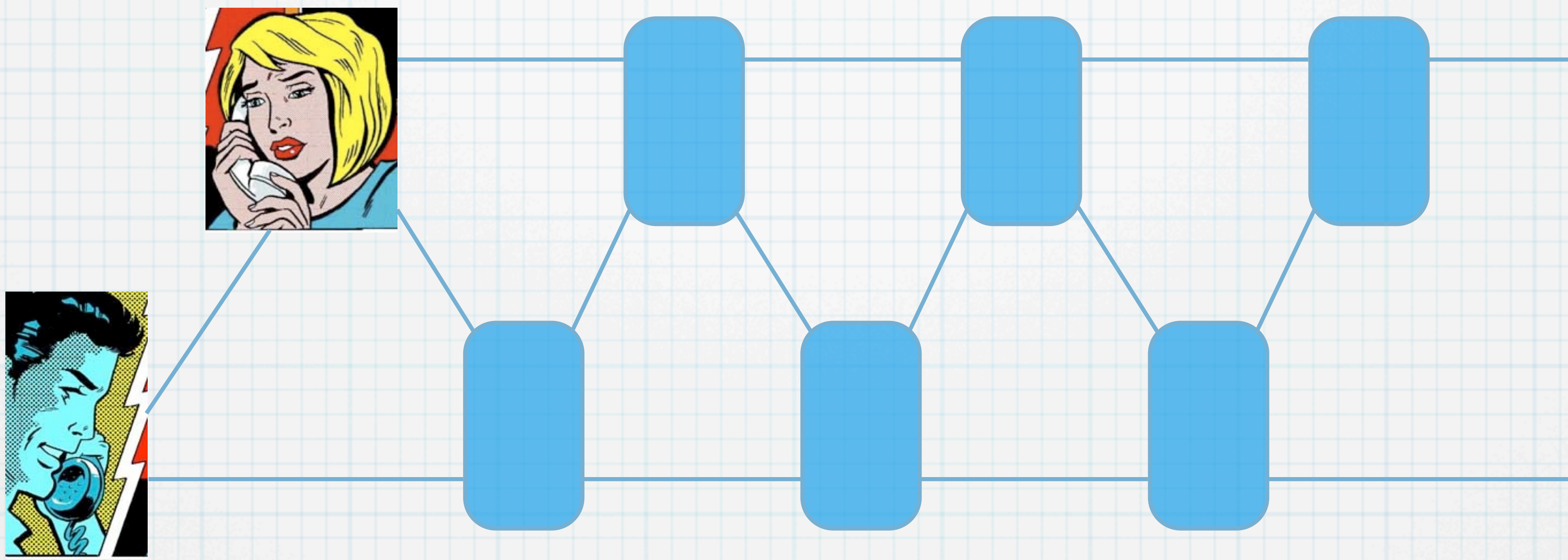
$$\Delta := C - D$$

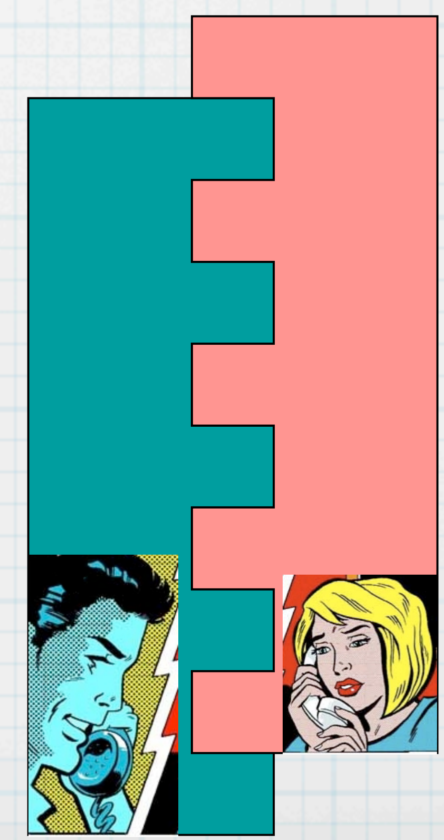
CB-norm distance only accounts for parallel discrimination schemes

QUit quantum information theory group

Application 2: quantum protocols (cryptography, game-theory)

Quantum protocols

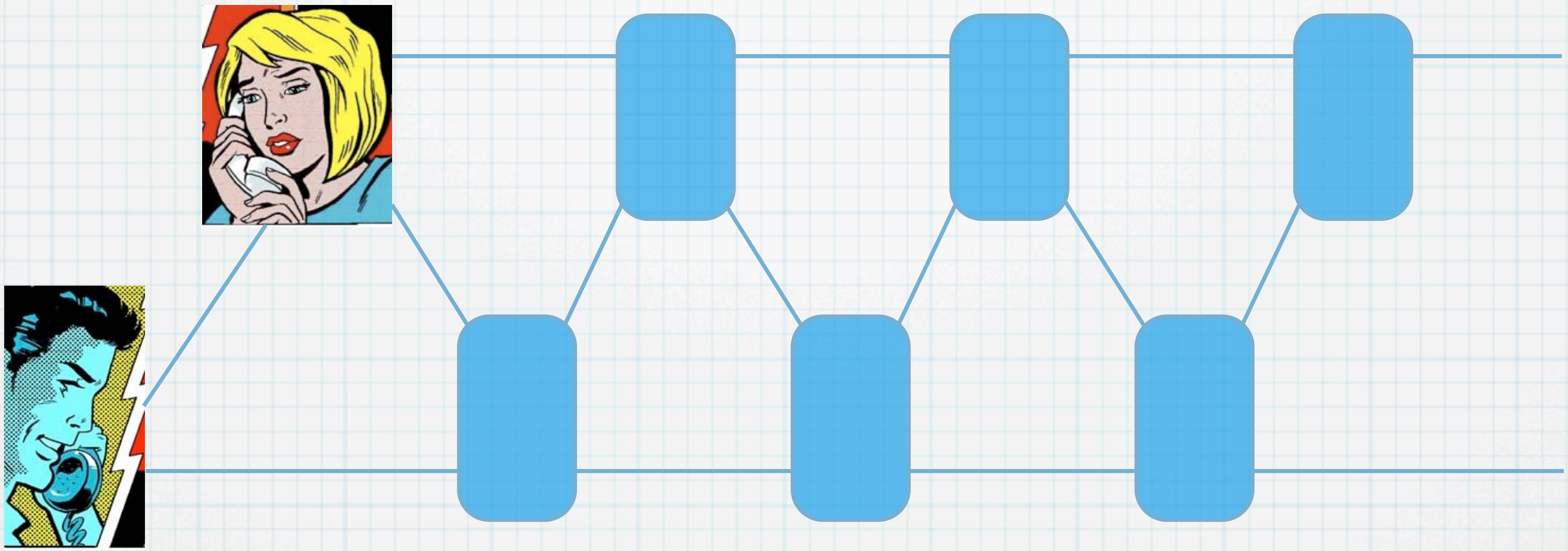




Quantum combs describe the most general strategies in multi-party protocols and games

G. Gutoski and J. Watrous, Proc. STOC, 565-574, (2007)

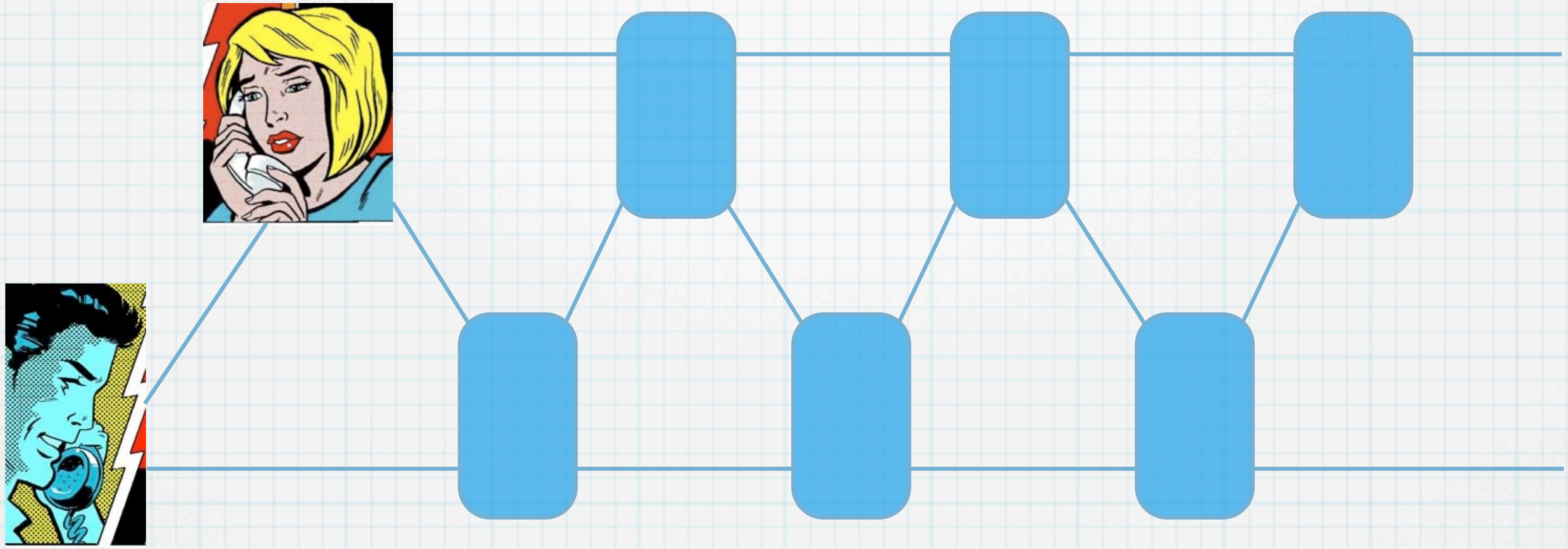
Quantum bit commitment



Quantum combs is the most suitable mathematical formulation of Alice and Bob’s strategies in a quantum bit commitment protocol

Sketch of impossibility proof

Chiribella, D'Ariano, Perinotti, Schlingemann, and Werner (in preparation)



Thm: a QBC concealing protocol cannot be binding

Proof: continuity of the comb-Stinespring versus the operational distance between strategies

Application 3: Quantum-algorithm learning

Quantum-algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

Quantum-algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

Quantum-algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- Alice owns quantum circuit that performs a very valuable algorithm U that she wants to keep undisclosed.

QUit quantum information theory group

Quantum-algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- Alice owns quantum circuit that performs a very valuable algorithm U that she wants to keep undisclosed.
- Bob needs to run Alice's algorithm on an input state that will be available tomorrow, but he can borrow the circuit from Alice only today for just a limited number of uses N, and with the circuit sealed.

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- The only thing that Bob can do today, with the circuit available, is to use it on a input state known to him.

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- The only thing that Bob can do today, with the circuit available, is to use it on a input state known to him.
- After that the only thing that remains available to Bob for tomorrow is the output state, which Bob can store on a quantum memory.

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- The only thing that Bob can do today, with the circuit available, is to use it on a input state known to him.
- After that the only thing that remains available to Bob for tomorrow is the output state, which Bob can store on a quantum memory.
- Therefore, Bob needs a quantum device that is capable of retrieving from the output state, namely recovering U and then running it on a new unknown state.

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

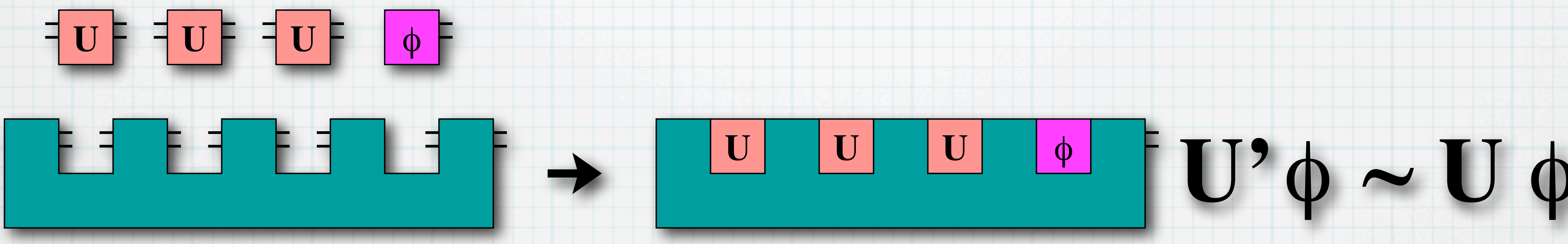
Quantum algorithm learning

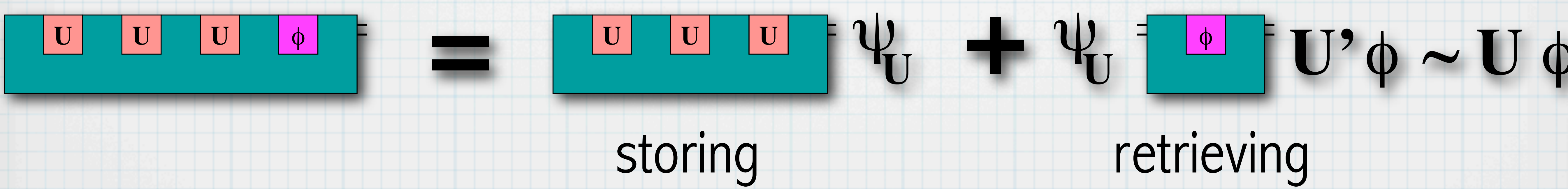
Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow

- Exact storing of quantum states is possible (quantum memory is a technological problem)
- Perfect storing of undisclosed unitaries over a quantum state is impossible even in-principle (Nielsen-Chuang no-programming theorem)

Quantum algorithm learning

Problem: run an unknown unitary that is available today on a quantum state that will be available tomorrow





Quantum algorithm learning

Problem: a black box computes an unknown function y = f(x)

We can evaluate f on a finite set of points $x_1, \ldots, x_N$

getting outcomes $y_1, \ldots, y_N$

Quantum algorithm learning

Problem: a black box computes an unknown function y = f(x)

We can evaluate f on a finite set of points $x_1, \dots, x_N$

getting outcomes $y_1, \dots, y_N$

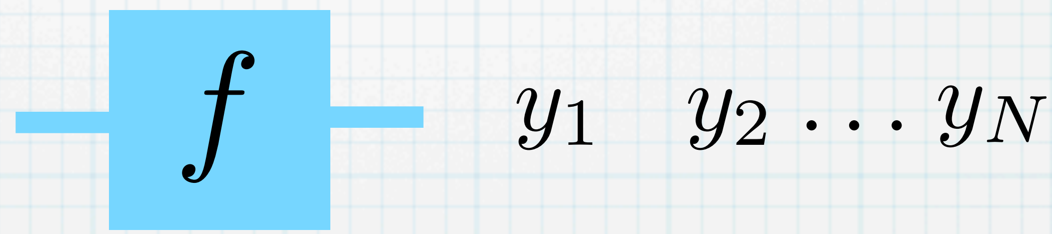
$y_1 \quad y_2 \cdots y_N$

Quantum algorithm learning

Problem: a black box computes an unknown function y = f(x)

We can evaluate f on a finite set of points $x_1, \ldots, x_N$

getting outcomes $y_1, \ldots, y_N$



Subsequently, we are asked to compute f on a new point x ,

without using the black box $f(x) = \ ?$

QUit quantum information theory group

Quantum algorithm learning

Problem: a black box computes an unknown function y = f(x)

We can evaluate f on a finite set of points $x_1, \ldots, x_N$

getting outcomes $y_1, \ldots, y_N$

$y_1 \quad y_2 \ldots y_N$

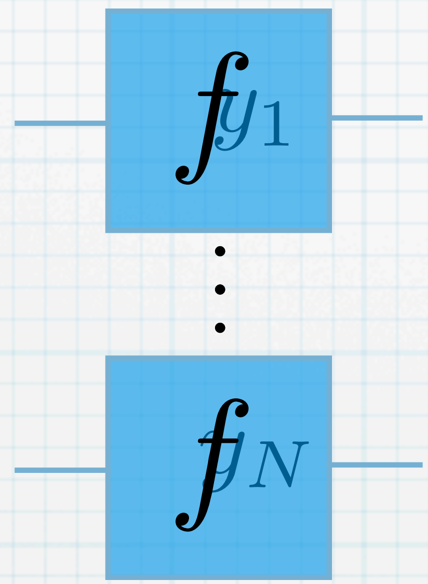
Subsequently, we are asked to compute f on a new point x , without using the black box $f(x) = \ ?$

In classical computer science, statistical learning provides a method to solve this problem

Quantum algorithm learning

classical networks for learning:

Comparing x with f(x) for N times is not the only possibility:
this just corresponds to the parallel configuration

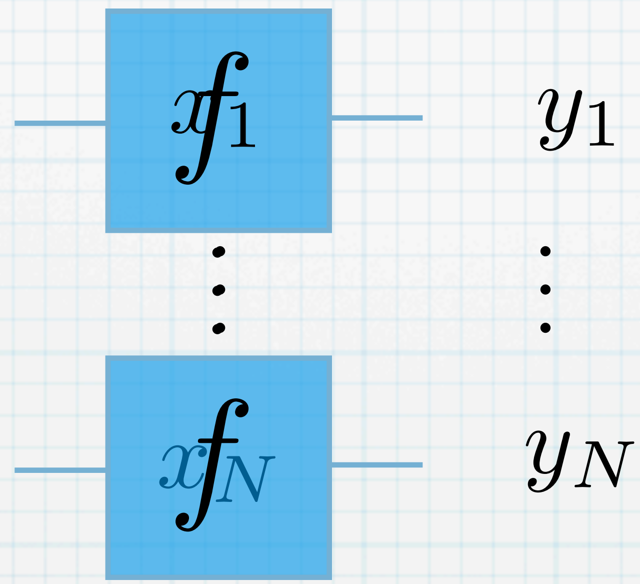


QUit quantum information theory group

Quantum algorithm learning

classical networks for learning:

Comparing x with f(x) for N times is not the only possibility:
this just corresponds to the parallel configuration

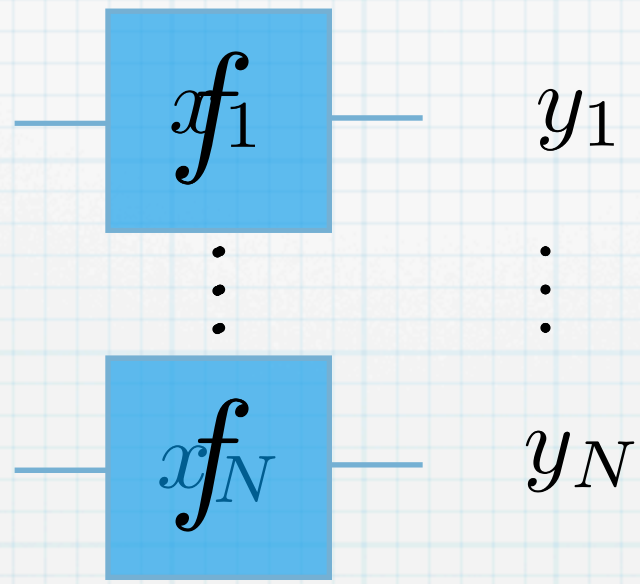


QUit quantum information theory group

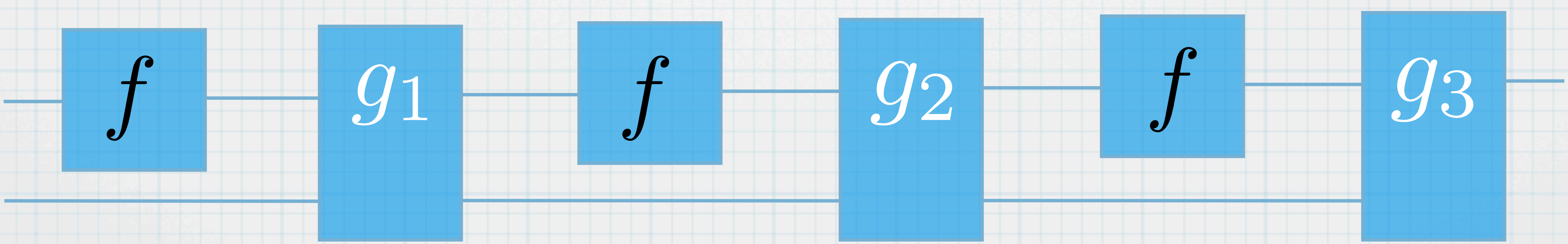
Quantum algorithm learning

classical networks for learning:

Comparing x with f(x) for N times is not the only possibility: this just corresponds to the parallel configuration



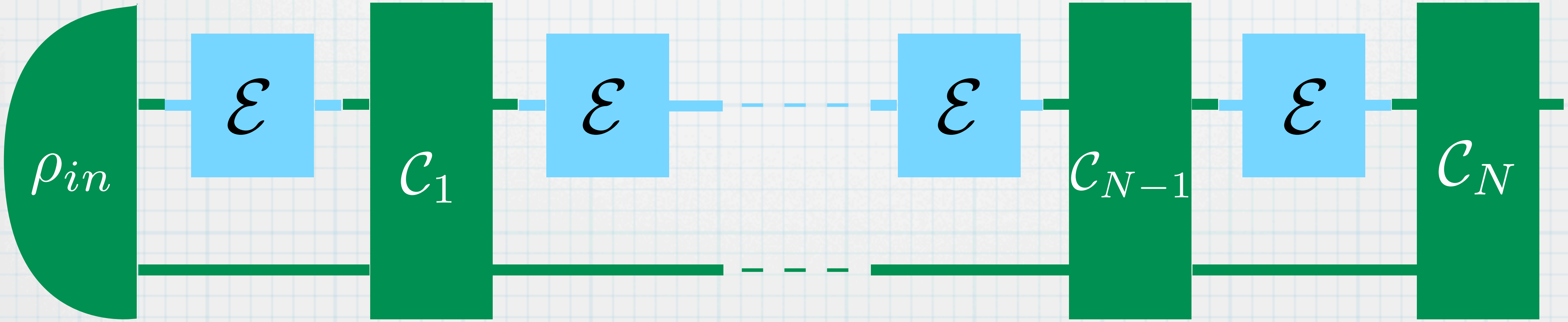
To learn better, one could use a sequential network:



where $g_1, g_2, \ldots, g_N$ are known functions

Quantum algorithm learning

- Unknown function f $\longrightarrow$ unknown quantum channel $\mathcal{E}$
- Classical program $\longrightarrow$ quantum network
- Input X $\longrightarrow$ quantum state ρ_{in}
- Output Y $\longrightarrow$ quantum state ρ_{out}



Quantum algorithm learning

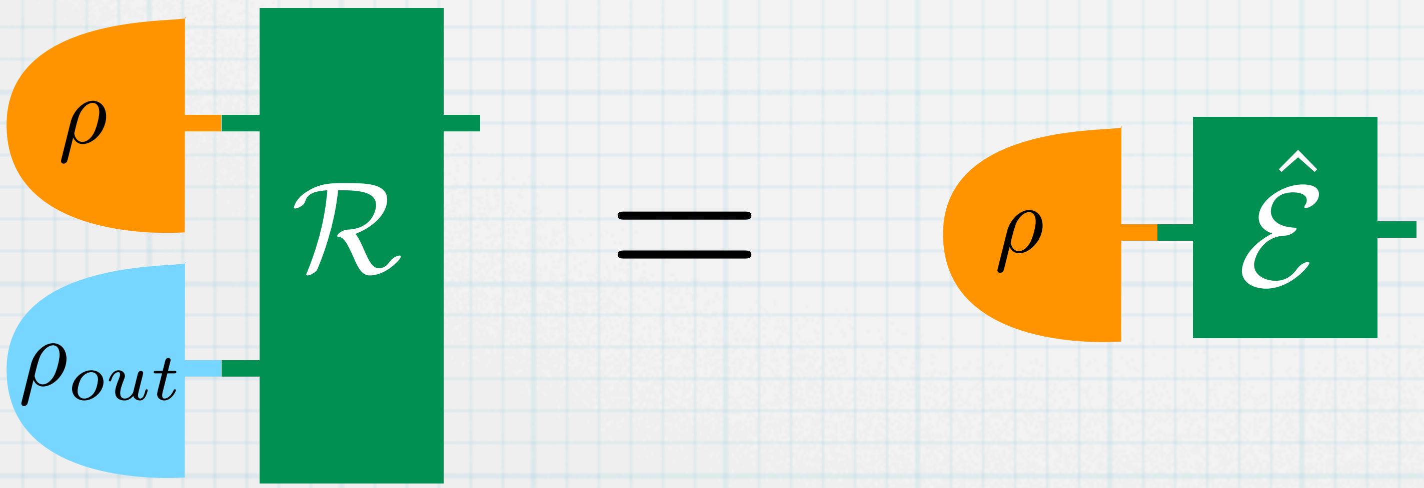
- Classical guess $\qquad\qquad\qquad\qquad$ Quantum “guess”

$$Y \to \hat{f} \qquad \longrightarrow \qquad \rho_{out} \to \hat{\mathcal{E}}$$

Physical implementation of the quantum guess:

retrieving channel $\mathcal{R}$

It retrieves the unknown transformation from the output state ρ_{out} and performs it on a new state ρ



Quantum algorithm learning

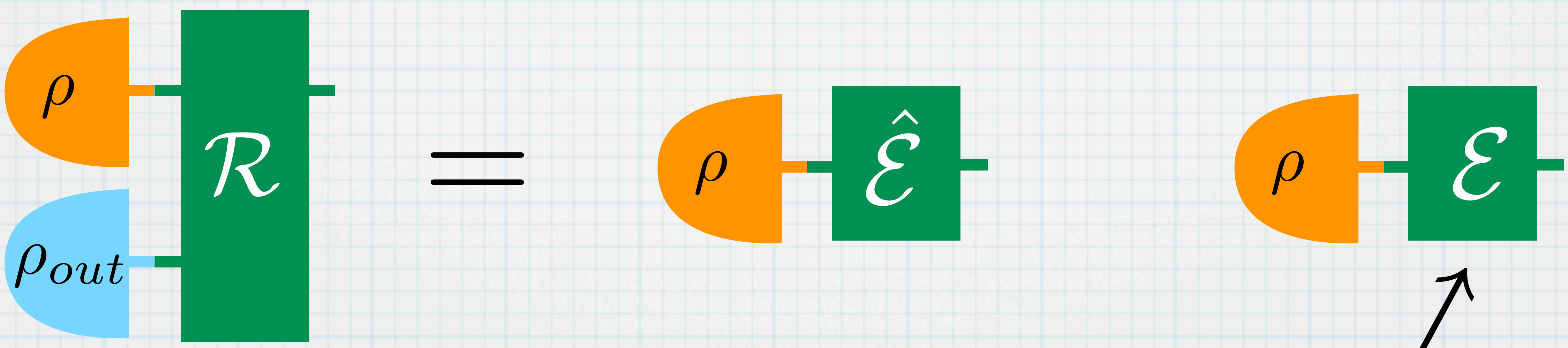
- Classical guess $\longrightarrow$ Quantum "guess"

$$Y \to \hat{f} \qquad\qquad\qquad \rho_{out} \to \hat{\mathcal{E}}$$

Physical implementation of the quantum guess:

retrieving channel $\mathcal{R}$

It retrieves the unknown transformation from the output state ρ_{out} and performs it on a new state ρ



Target: implementing the unknown channel with maximum fidelity

Quantum algorithm learning

find the optimal quantum comb

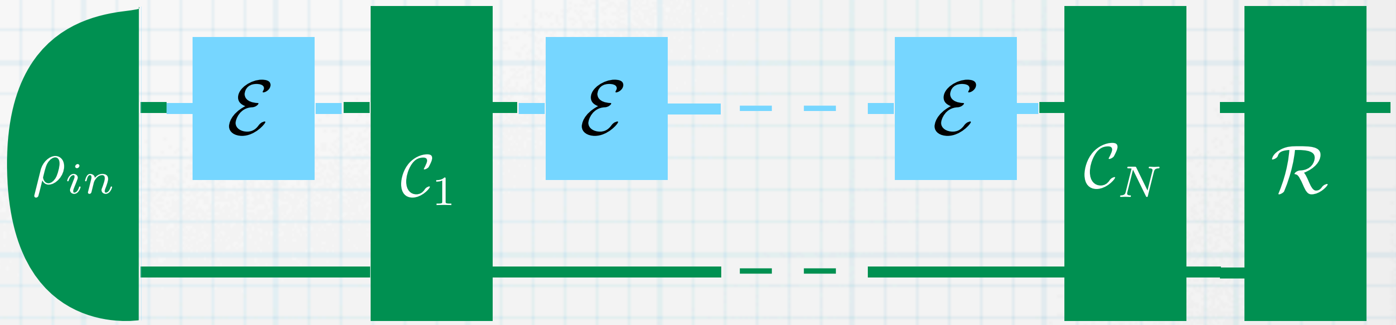
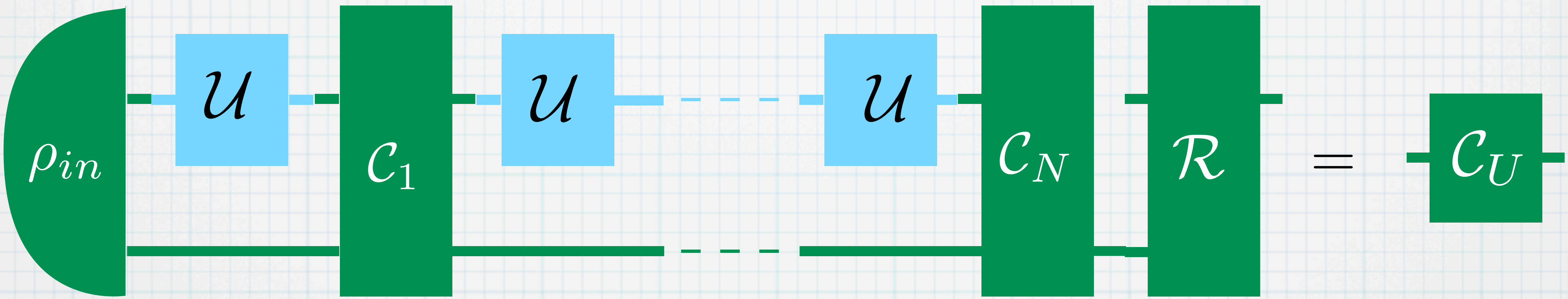


Figure of merit: input-output fidelity

$$F(\mathcal{E}, \hat{\mathcal{E}}) = \int \mathrm{d}\varphi \;\; F(\mathcal{E}(\varphi), \hat{\mathcal{E}}(\varphi)) \qquad F(\rho, \sigma) = \mathrm{Tr}\left[(\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}})^{\frac{1}{2}} \right]$$

Quantum algorithm learning

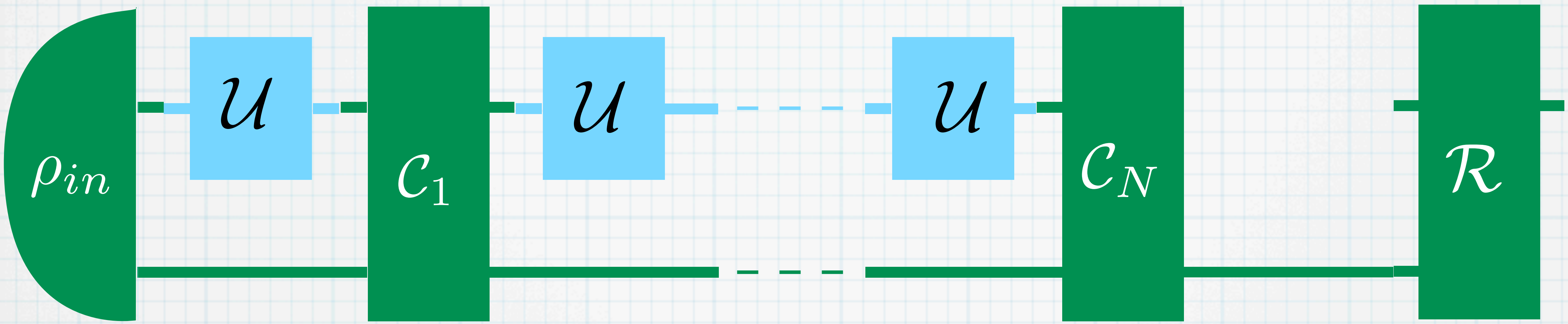
Consider the case where the set of channels is a group of unitary transformations.



Assuming a uniform prior for the unknown unitaries, we have the average fidelity

$$F = \int \mathrm{d}U \quad F(\mathcal{U}, \mathcal{C}_U)$$

Quantum algorithm learning



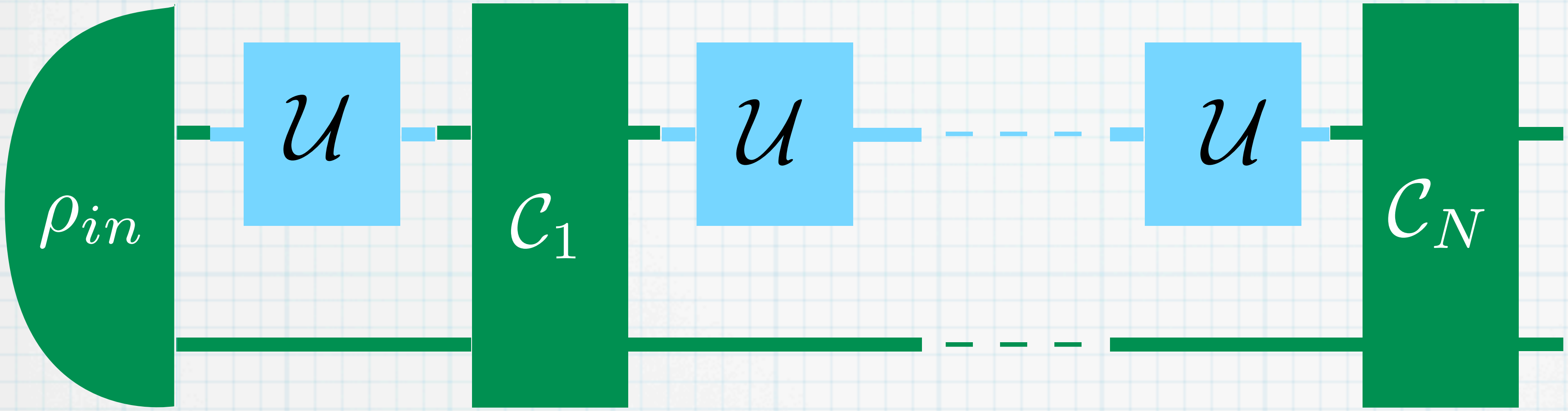
Comb of the learning network: $L = R * C_N * \cdots * C_2 * C_1 * \rho_{in}$

Fidelity: $$F = \frac{1}{d^2} \int \mathrm{d}U \ \ \langle\langle U | \langle\langle U^* |^{\otimes N} | \ L \ | U \rangle\rangle | U^* \rangle\rangle^{\otimes N}$$

We can always optimize over covariant combs:

$$[L, U \otimes V^* \otimes U^{* \otimes N} \otimes V^{\otimes N}] = 0 \qquad \forall U, V$$

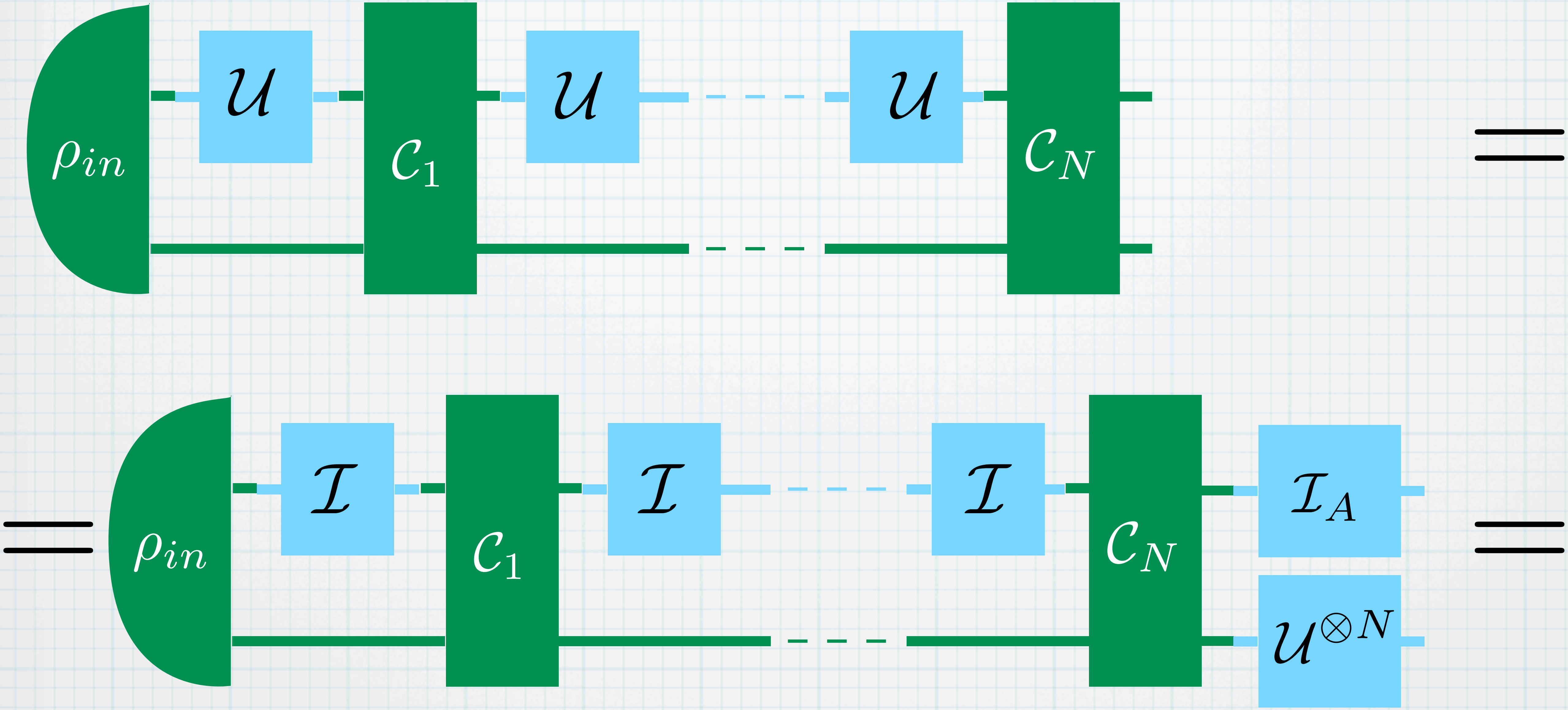
Quantum algorithm learning



$=$

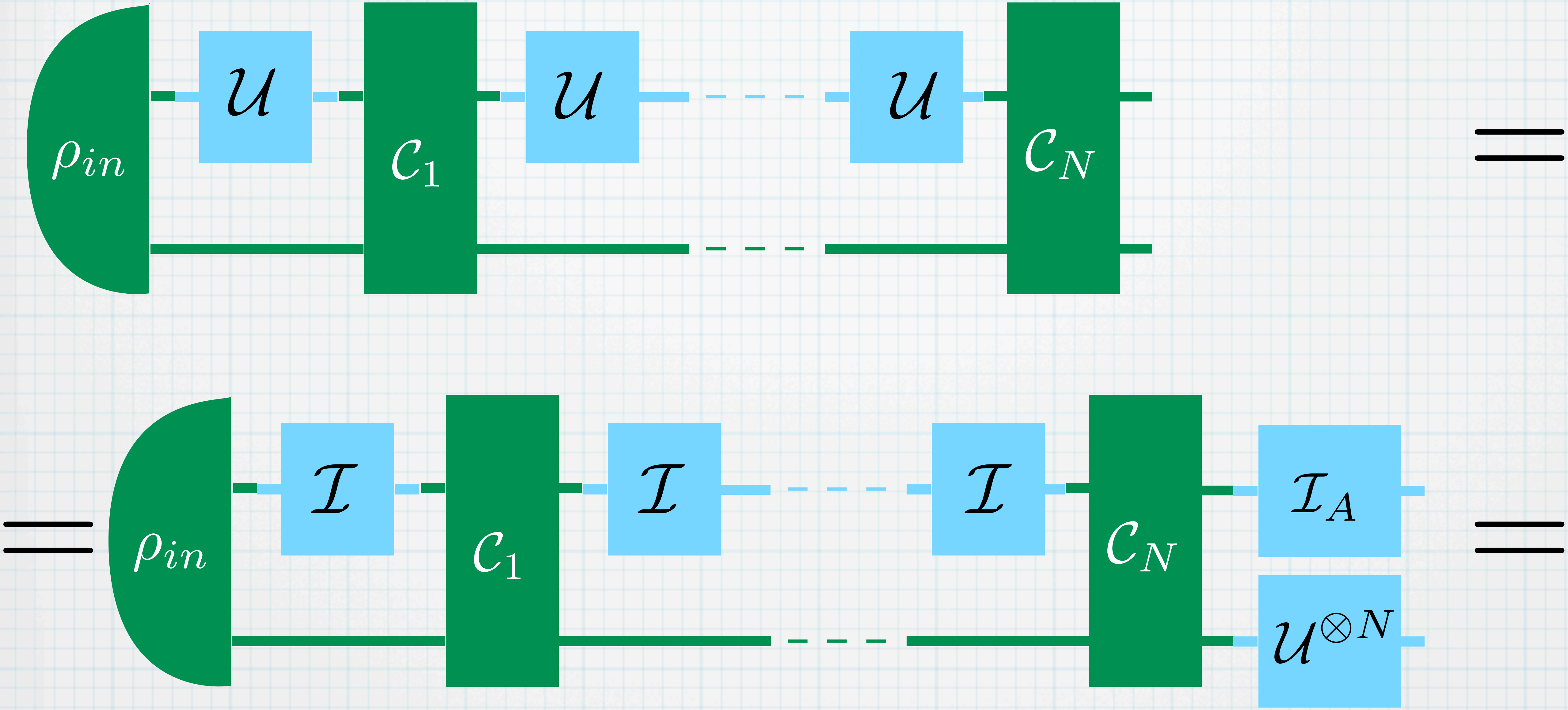
QUit quantum information theory group

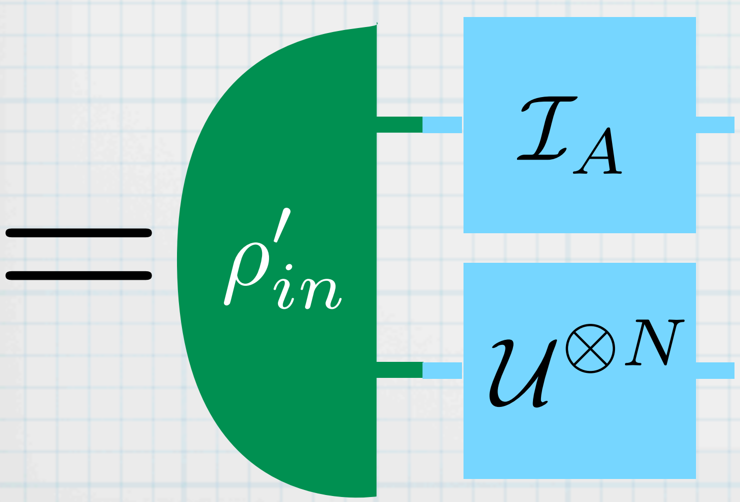
Quantum algorithm learning



QUit quantum information theory group

Quantum algorithm learning





Any covariant network is equivalent to a parallel scheme with ancilla!

Learning can be parallelized, in the same way as estimation

Quantum algorithm learning

Decomposing the unitaries as $$U^{\otimes N} \otimes I_A = \bigoplus_J (U_J \otimes I_{m_J})$$

one can prove that the optimal input states have the form

$$|\psi\rangle = \bigoplus_J a_J \frac{|I_J\rangle\rangle}{\sqrt{d_J}} \qquad a_J \geq 0$$

where $|I_J\rangle\rangle \in \mathcal{H}_J^{\otimes 2}$ is a maximally entangled state

This is the same form of the optimal states for
estimation of the unknown unitary U with N copies

G Chiribella, G M D'Ariano, and M F Sacchi, Phys. Rev. A 72, 043448 (2005).

Quantum algorithm learning

Bisio, Chiribella, D'Ariano, Facchini, Perinotti (unpublished)

Theorem: for any group of unitaries, for an input state of the optimal form

$$|\psi\rangle = \bigoplus_J a_J \frac{|I_J\rangle\rangle}{\sqrt{d_J}} \qquad a_J \geq 0$$

the optimal retrieving channel to extract U from the states

$$(U^{\otimes N} \otimes I_A)|\psi\rangle = \bigoplus_J a_J \frac{|U_J\rangle\rangle}{\sqrt{d_J}} \qquad a_J \geq 0$$

is achieved by a "measure-and-prepare" scheme.

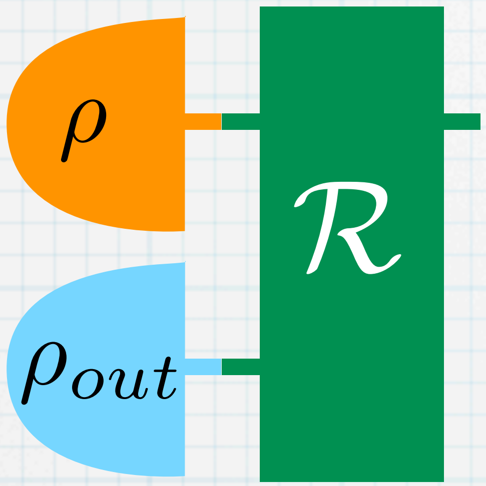
(estimation of the unknown unitary U:

for outcome $\hat{U}$, just perform the unitary $\hat{U}$)

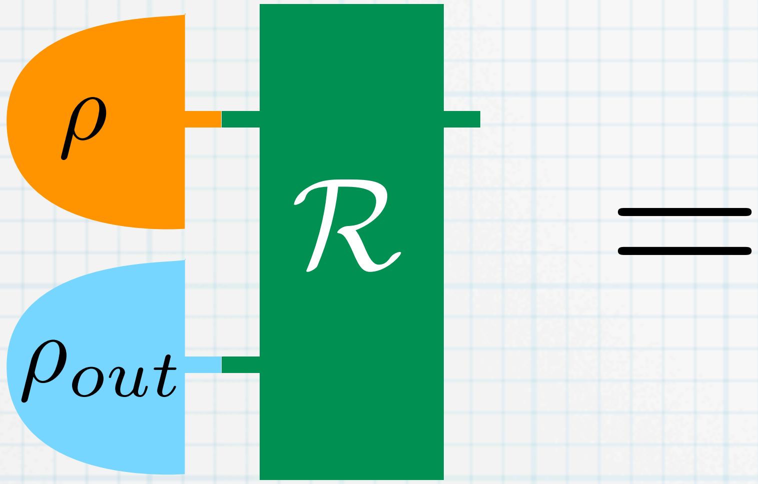
For the optimal POVM, see G Chiribella, G M D'Ariano, and M F Sacchi, Phys. Rev. A 72, 043448 (2005).

Quantum algorithm learning

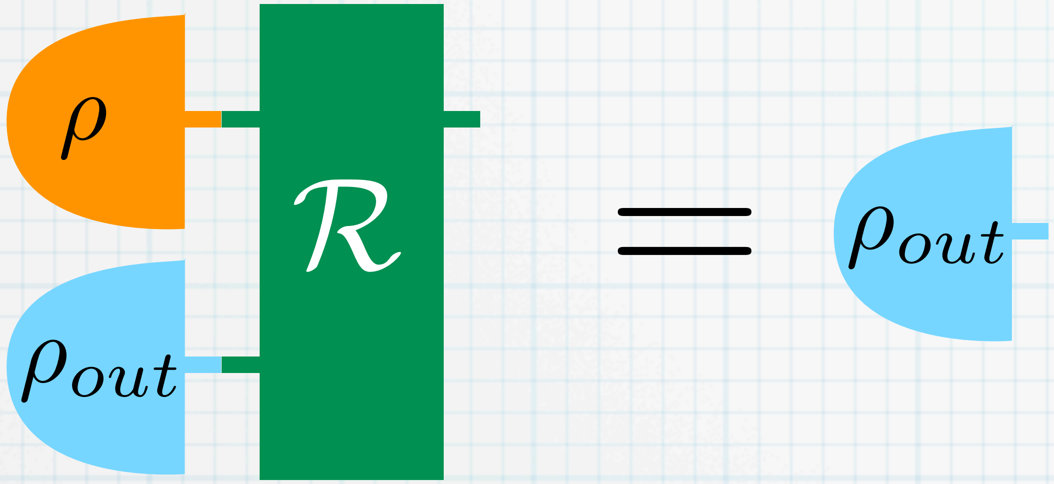
Quantum algorithm learning



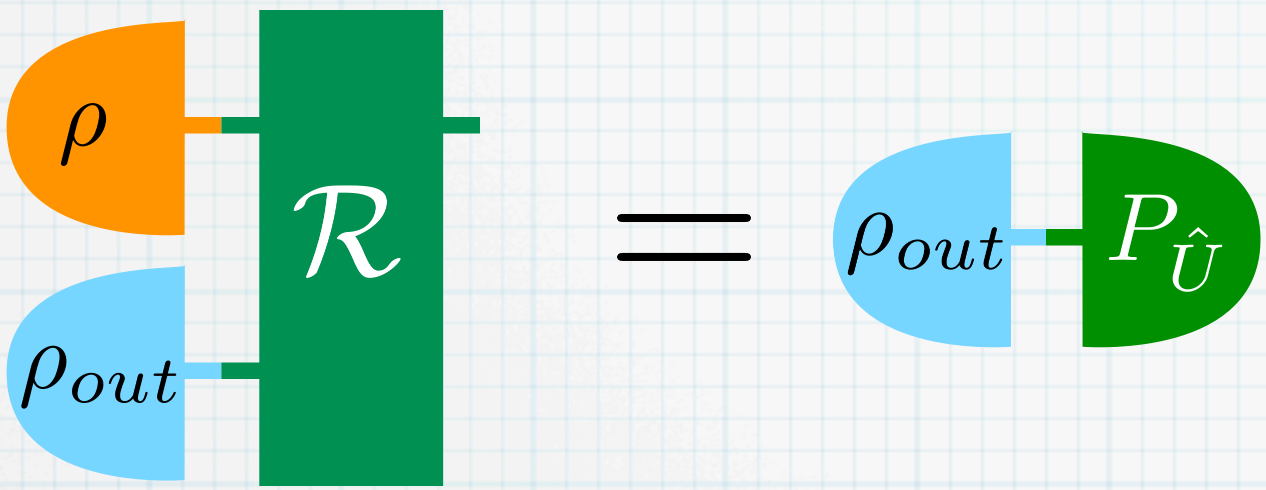
Quantum algorithm learning



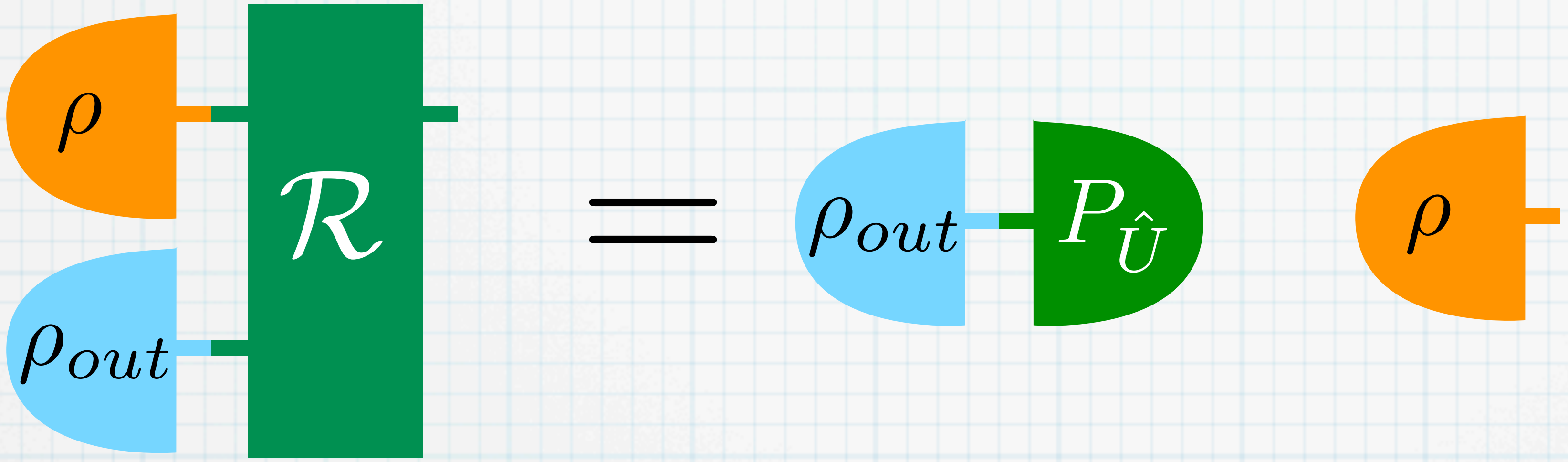
Quantum algorithm learning



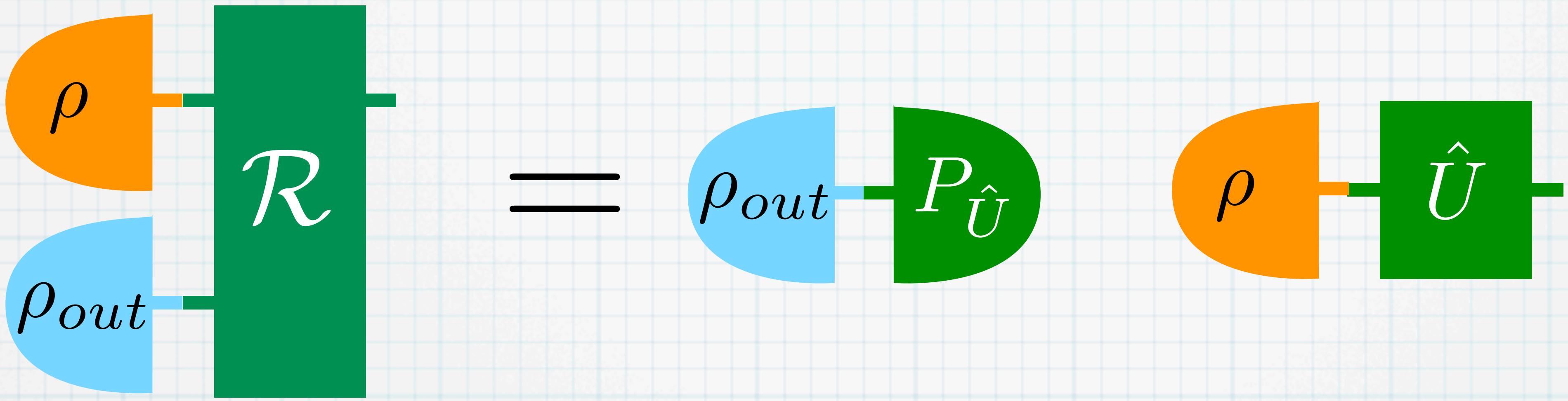
Quantum algorithm learning



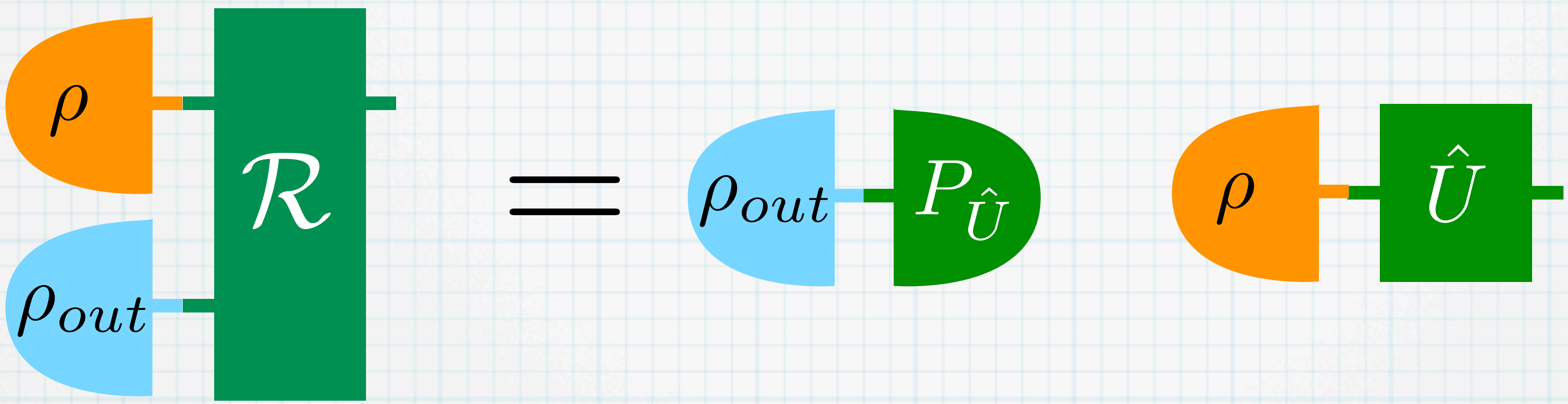
Quantum algorithm learning



Quantum algorithm learning



Quantum algorithm learning

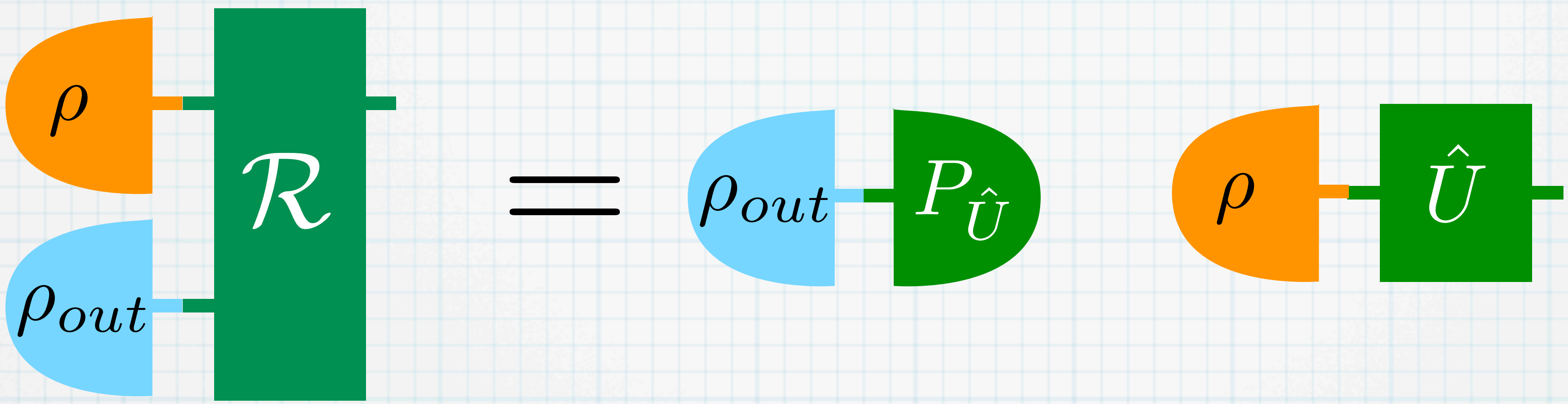


Optimal retrieving is “measure-and-prepare”: no need for quantum memory. We can measure immediately after applying U, and store the outcome $\hat{U}$ in a classical memory.

We can make as many copies as we want (a quantum memory is degraded at every access).

QUit quantum information theory group

Quantum algorithm learning



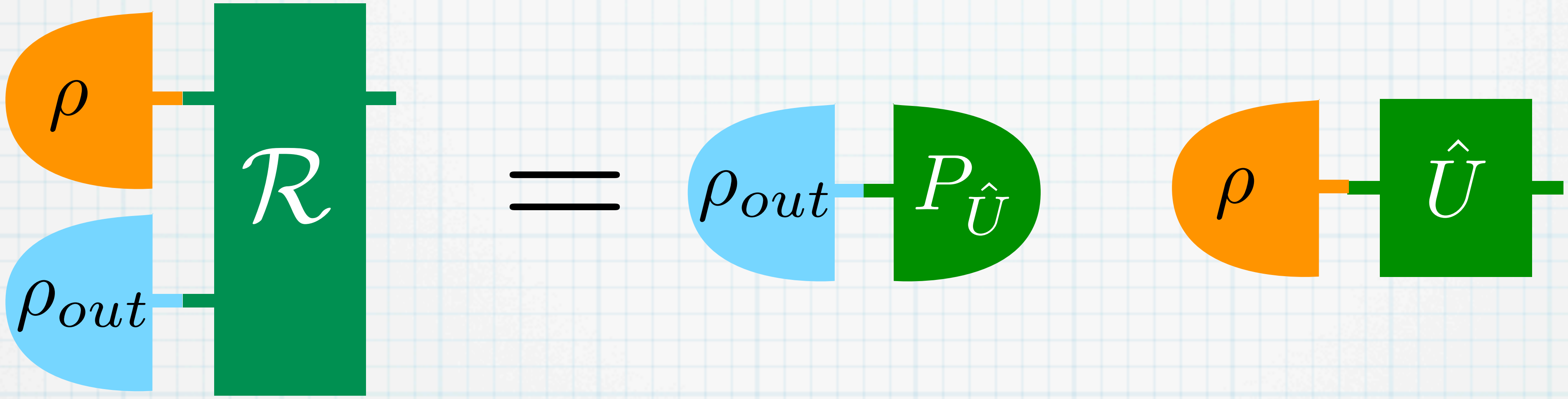
Optimal retrieving is "measure-and-prepare": no need for quantum memory. We can measure immediately after applying U, and store the outcome $\hat{U}$ in a classical memory.

We can make as many copies as we want (a quantum memory is degraded at every access).

Parallel scheme + measure&reprepare still optimal for:

- N non-identical input unitaries (and/or non-identical target unitaries)
- perform the inverse of U: target $U^\dagger$ (error correction with correlated noise)

Quantum algorithm learning



Optimal retrieving is "measure-and-prepare": no need for quantum memory. We can measure immediately after applying U, and store the outcome $\hat{U}$ in a classical memory.

We can make as many copies as we want (a quantum memory is degraded at every access).

Parallel scheme + measure&reprepare still optimal for:

- N non-identical input unitaries (and/or non-identical target unitaries)
- perform the inverse of U: target $U^\dagger$ (error correction with correlated noise)

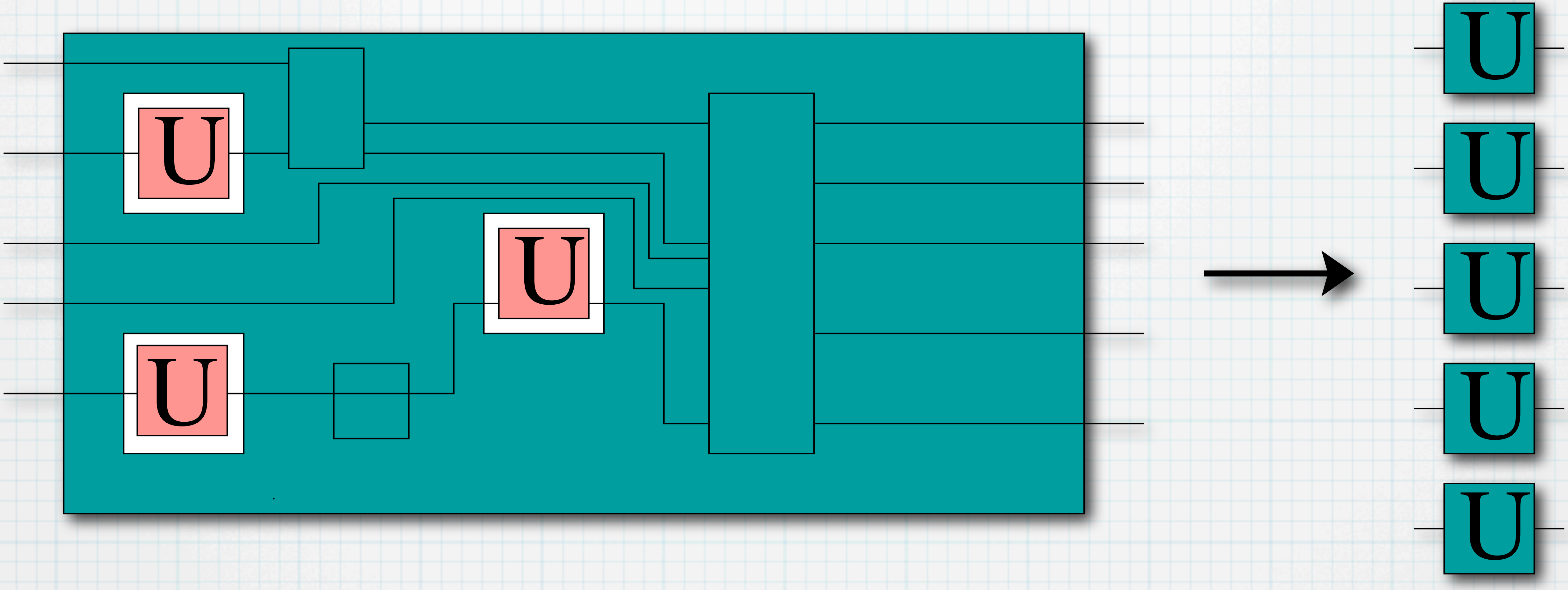
not necessarily optimal for

- learning general channels
- learning unitaries that do not form a group
- learning with restrictions on the available input states (entanglement)

Application 4: Optimal cloning of unitaries

Cloning of unitaries

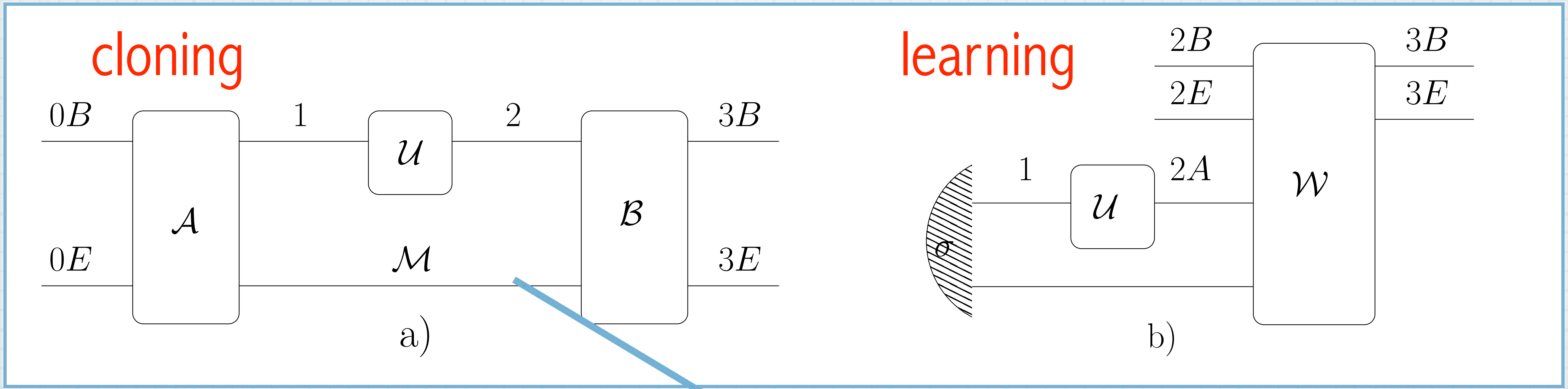
G. Chiribella, G. M. D'Ariano, P. Perinotti PRL **101** 180504 (2008)



$$F = \int \mathrm{d}U \, F(\mathscr{T}_U^{(N)}, \mathscr{T}_U^{\otimes N})$$ (channel fidelity)

Cloning of unitaries

Chiribella, D'Ariano, Perinotti, PRL **101** 180504 (2008)



(same for learning)

1-to-2 cloning $$F = \frac{d + \sqrt{d^2 - 1}}{d^3} > F_{est} = \frac{6}{d^4} (d \neq 2)$$

Much better than cloning states $(I \otimes U)|I\rangle\rangle$ → q-learning

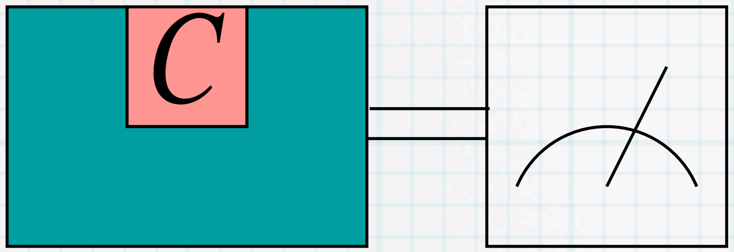
Applying U to a state "degrades" U

Cloning unitaries is harder than cloning states (cryptography with information encoded on transformations is more secure)

QUit quantum information theory group

Application 5: Optimal quantum tomography

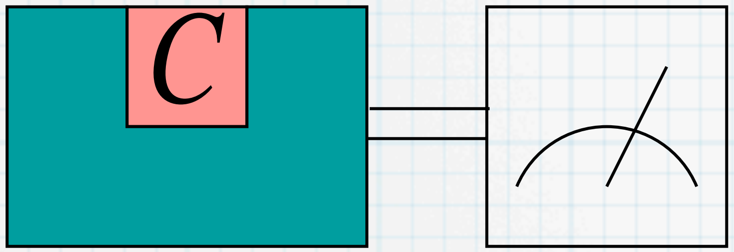
Optimal tomographers



(d^4 outcomes)

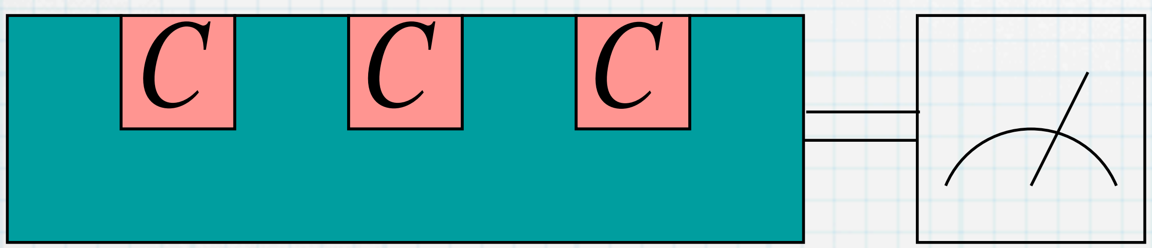
Informationally complete tester

Optimal tomographers



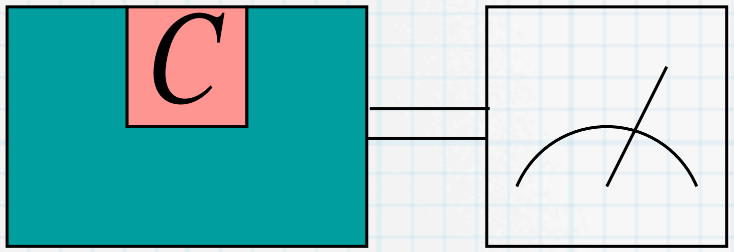
(d^4 outcomes)

Informationally complete tester



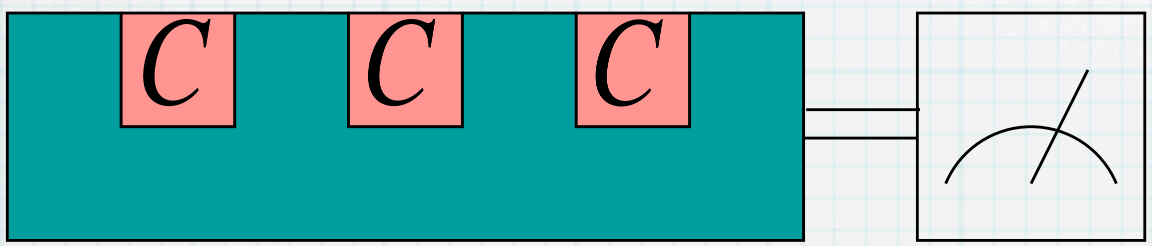
multiple uses

Optimal tomographers

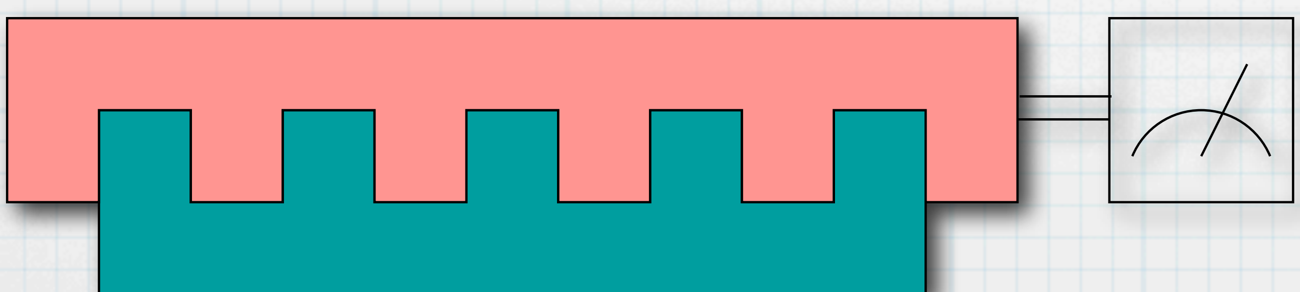


(d^4 outcomes)

Informationally complete tester



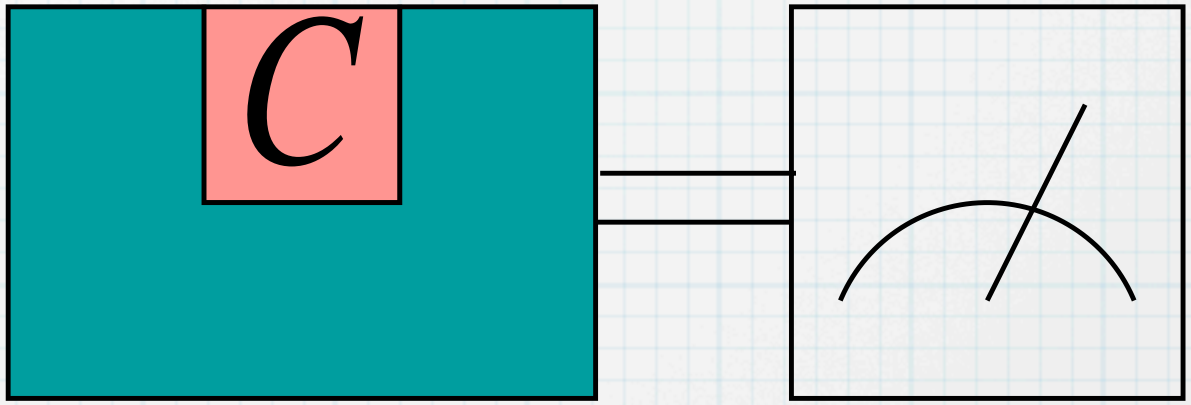
multiple uses



circuit board tomographer

Optimal tomography

Use different in and out dimensions to unify: states, channels, and POVMs

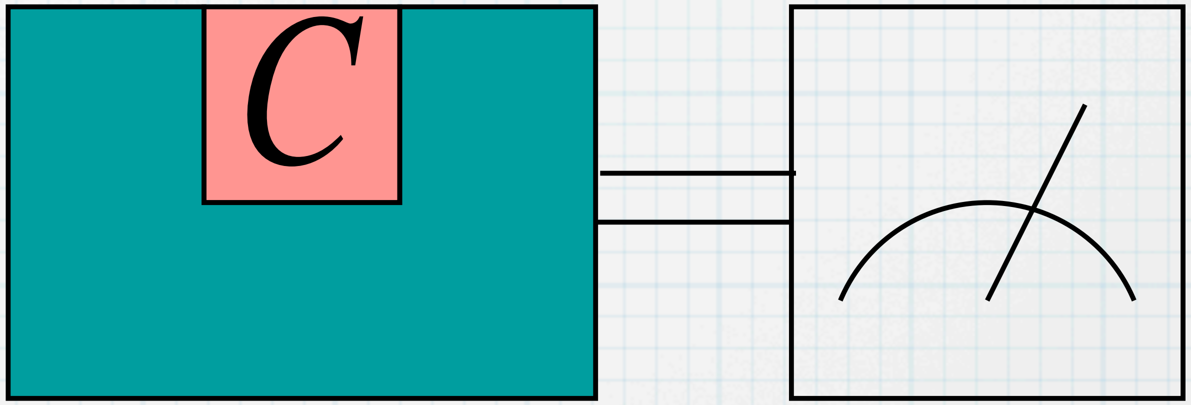


A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti PRL 102 010404 (2009) arXiv: 0806.1172

Optimal tomography

- Prior distribution of channels corresponding to the depolarizing average channel
- Cost function = representation, (equally weighted orthonormal set of operators)
- Further selection:
  1) quantum operations,
  2) channels,
  3) unital channels

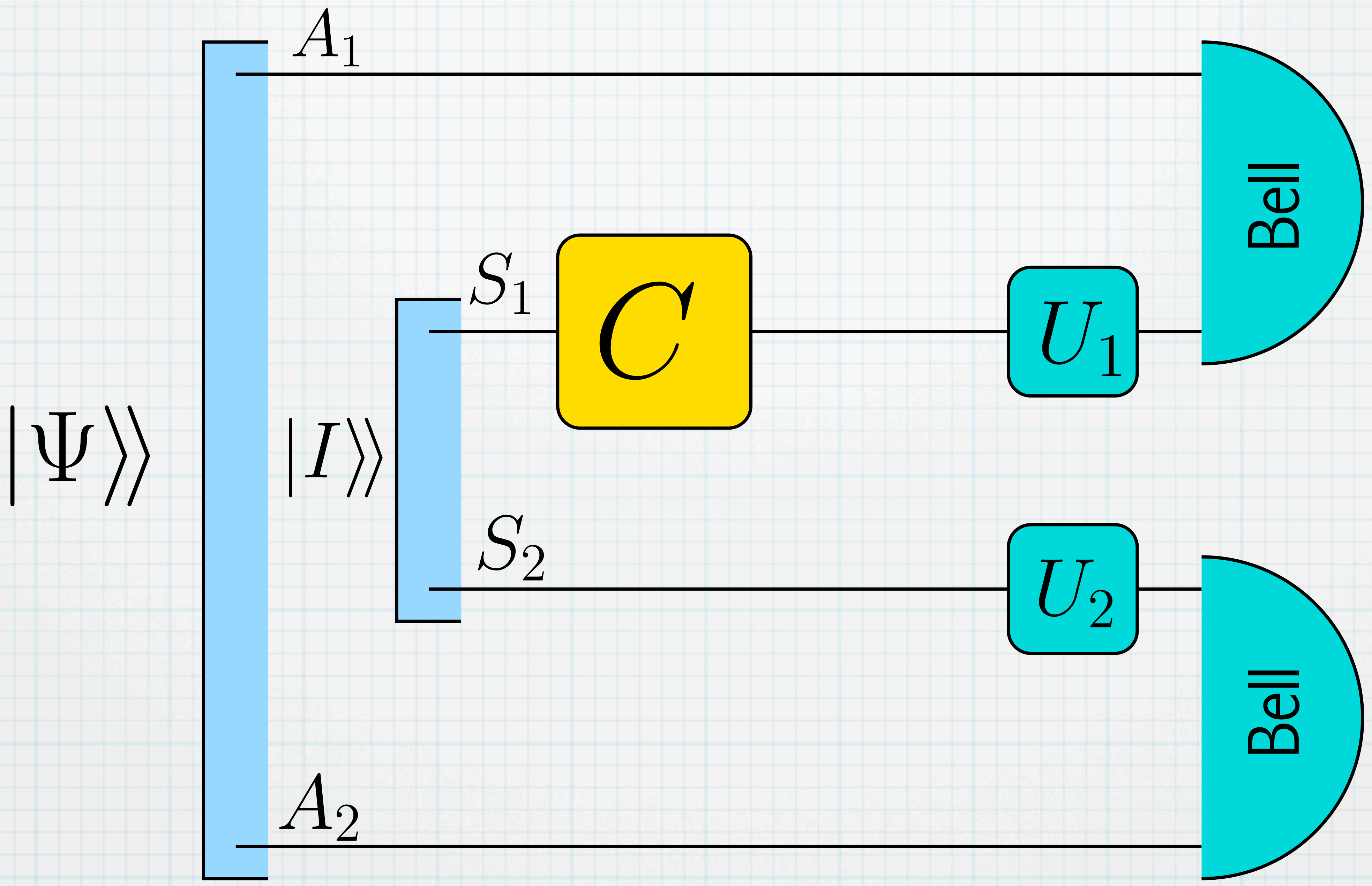
Use different in and out dimensions to unify: states, channels, and POVMs



A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti PRL 102 010404 (2009)

arXiv: 0806.1172

Optimal tomography



$$\Psi = [d^{-1}(1-\beta)I + \beta\,|\psi\rangle\langle\psi|]^{\frac{1}{2}}$$

$\beta = \sqrt{(d+1)/(d^2+1)}$ quantum operations

$\beta = [(d-1)(2+\sqrt{2}(d^2-1))]^{-1/2}$ channels

$\beta = 0$ unital channels

QUit quantum information theory group

Conclusions

PRL **101** 060401 (2008)
PRL **101** 180501 (2008)
PRL **101** 180504 (2008)
PRL **102** 010404 (2009)
EL **83** 30004 (2008)

Conclusions

PRL **101** 060401 (2008)
PRL **101** 180501 (2008)
PRL **101** 180504 (2008)
PRL **102** 010404 (2009)
EL **83** 30004 (2008)

- New Quantum Estimation Theory, with multiple copies, and optimization of the setup → optimization of quantum circuits architecture, engineering high-precision operations
  - Quantum circuit board = quantum comb = supermap
  - Comb algebra (link-product)
  - Convex optimization method
- Applications:
  - discrimination/estimation of unitaries and memory channels (optimal quantum oracle-calling algorithms)
  - quantum protocols
  - quantum-algorithm learning = storing undisclosable unitaries
  - cloning undisclosable unitaries
  - process tomography