Estimation and discrimination of quantum networks

Paolo Perinotti

in collaboration with
G. Chiribella and G. M. D'Ariano

DEX-SMI Workshop on Quantum Statistical Inference, 4 March 2009 NII, Tokyo

Summary

- Quantum combs: the theory of quantum networks
- Testers: measurements of network parameters
- Four results in quantum network estimation
    - Optimal discrimination of two transformations
    - Optimal covariant estimation of unitary channels
    - Optimal tomography
    - Analysis of Quantum Bit Commitment

Quantum channels

A quantum channel is a linear trace-preserving CP map

It is useful to represent quantum channels via their Choi operator

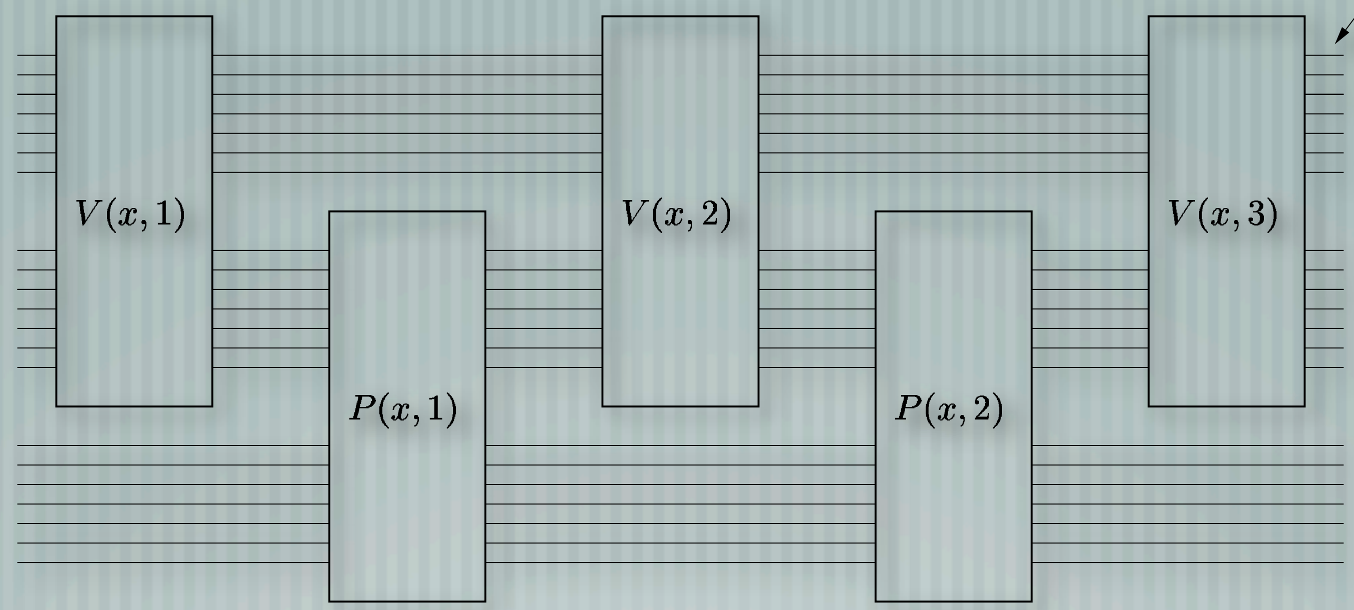
$$C := (\mathscr{C} \otimes \mathscr{I})(|\Omega\rangle\langle\Omega|), \quad \mathcal{H}_{\mathrm{out}} \otimes \mathcal{H}_{\mathrm{in}} \ni |\Omega\rangle := \sum_n |n\rangle|n\rangle$$

$$\Updownarrow$$

$$\mathscr{C}(\rho) = \mathrm{Tr}_{\mathrm{in}}[(I \otimes \rho^T)C]$$

TRACE PRESERVATION CONDITION $\quad \mathrm{Tr}_{\mathrm{out}}[C] = I_{\mathrm{in}}$

Quantum networks

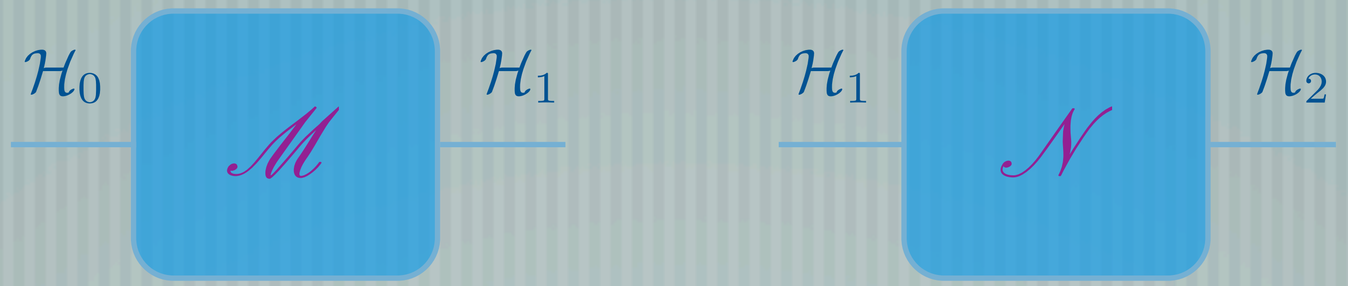


We want to describe quantum networks

What is the Choi operator of a network?

We start from 2 channels: $-\boxed{\mathscr{C}_1}-\boxed{\mathscr{C}_2}- \; = \; -\boxed{\mathscr{C}_3}-$

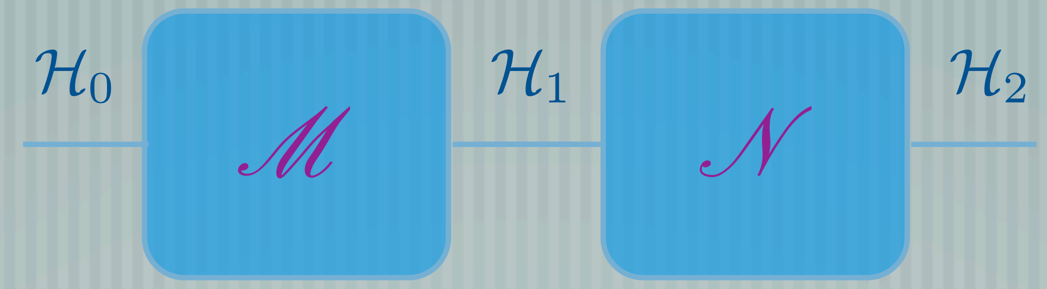
Link product



The definition of link product provides the Choi operator of the composed channel

$$L = M * N := \mathrm{Tr}_{\mathcal{H}_1}[(M \otimes I_0)(I_2 \otimes N^{\theta_1})]$$

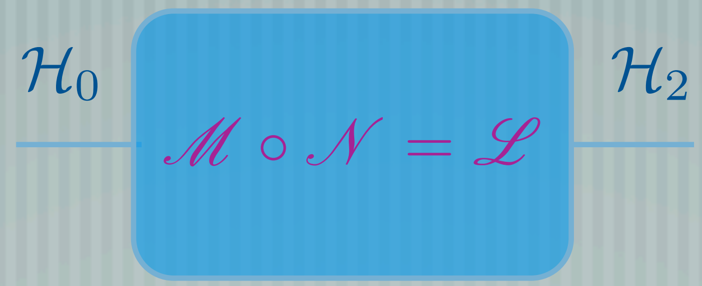
Link product



The definition of link product provides the Choi operator of the composed channel

$$L = M * N := \mathrm{Tr}_{\mathcal{H}_1}[(M \otimes I_0)(I_2 \otimes N^{\theta_1})]$$

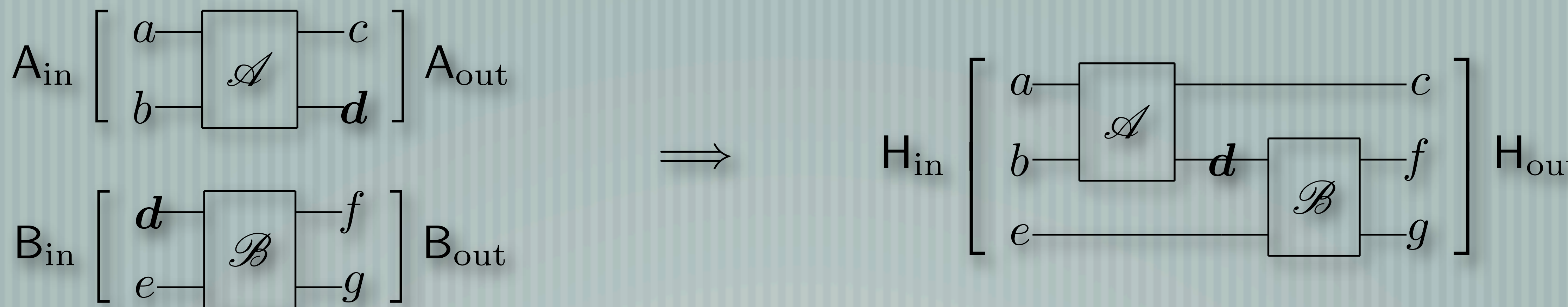
Link product



The definition of link product provides the Choi operator of the composed channel

$$L = M * N := \mathrm{Tr}_{\mathcal{H}_1}[(M \otimes I_0)(I_2 \otimes N^{\theta_1})]$$

Link product



$$\mathsf{J} = \mathcal{H}_d$$

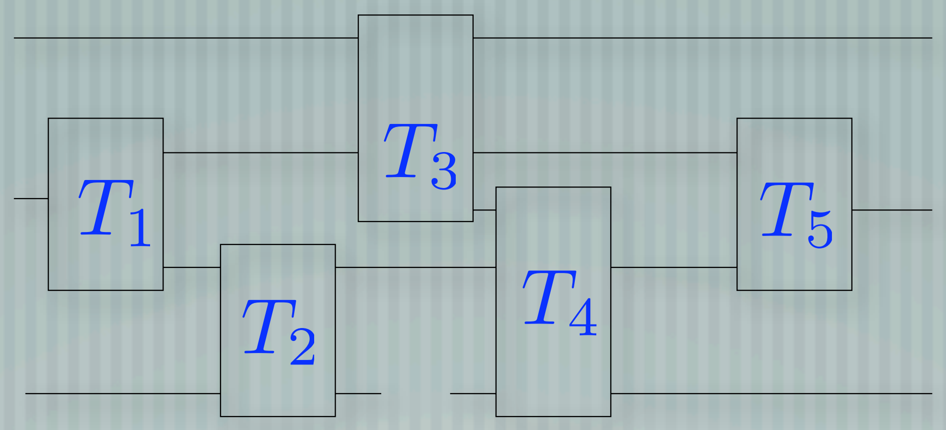
Choi-operator calculus

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

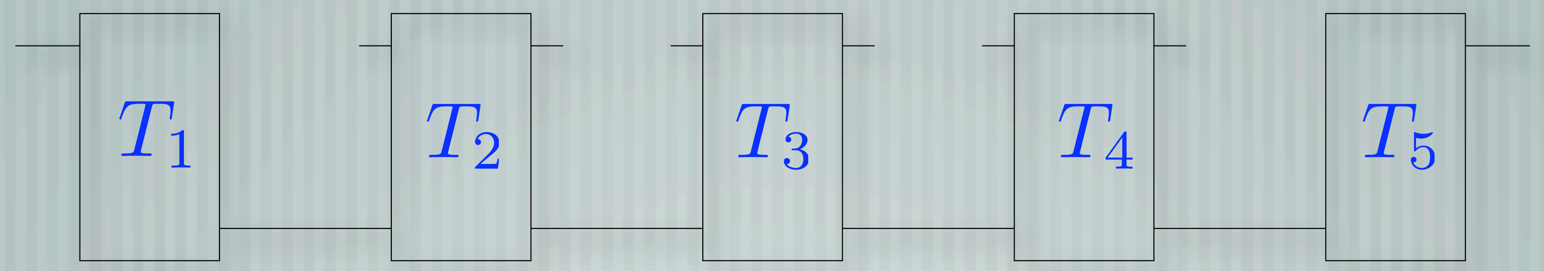
$$AB := (A_{a,b,c,d} \otimes I_{e,f,g})(I_{a,b,c} \otimes B_{d,e,f,g})$$

G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 060401 (2008).

Networks as combs



All networks can be sorted to form of a “comb network”

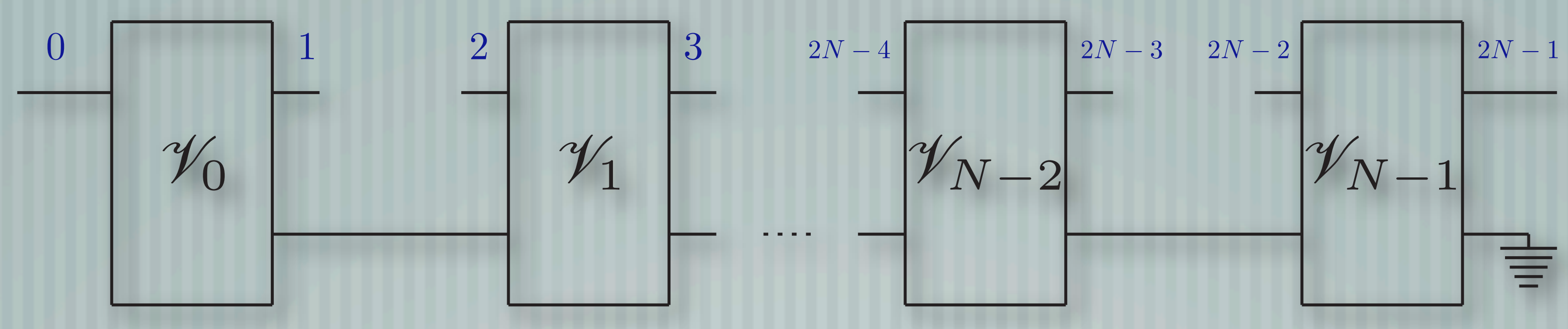


$$R = T_1 * T_2 * T_3 * T_4 * T_5$$

G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 060401 (2008).

The quantum comb

We consider networks of this kind



One can prove that the Choi operator of the network satisfes

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

$$R^{(0)} = 1$$

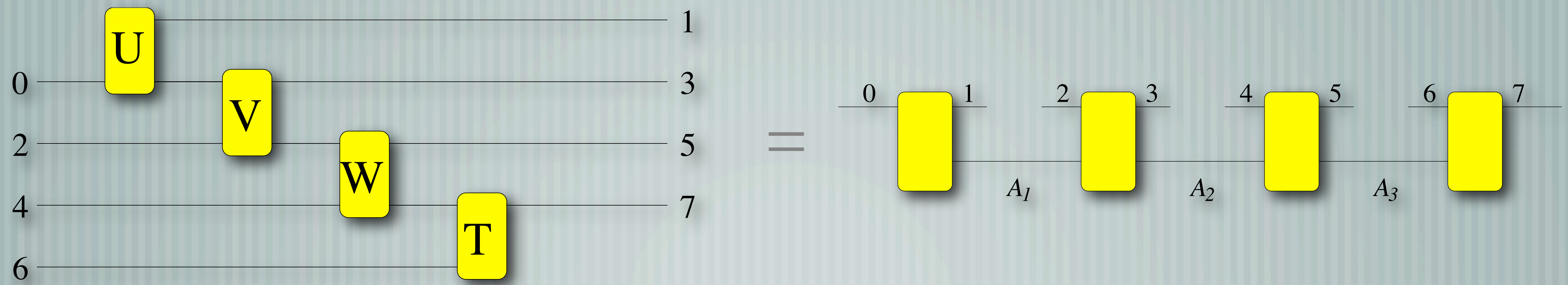
Realisation theorem

Also the converse is true: if R satisfies

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

$$R^{(0)} = 1$$

then it has a realisation scheme as a comb



G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 060401 (2008).

G. Chiribella, G. M. D'Ariano, and P. P., in preparation.

Testers

We consider networks of this kind

Their Choi operator is T_i and satisfies $\sum_i T_i = T = I_{2N-2} \otimes \Xi$

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

$$\Xi^{(N-1)} = \Xi, \quad I_0 = 1$$

$$R * T_i = \mathrm{Tr}[R T_i^T] = p(i|R), \quad \sum_i p(i|R) = 1$$

Realisation theorem

Also the converse is true: if T_i satisfies $\sum_i T_i = I_{2N-2} \otimes \Xi$

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

$$\Xi^{(N-1)} = \Xi, \quad I_0 = 1$$

then for all R $R * T_i = \mathrm{Tr}[R T_i^T] = p(i|R), \quad \sum_i p(i|R) = 1$

and the operators T_i correspond to a tester network

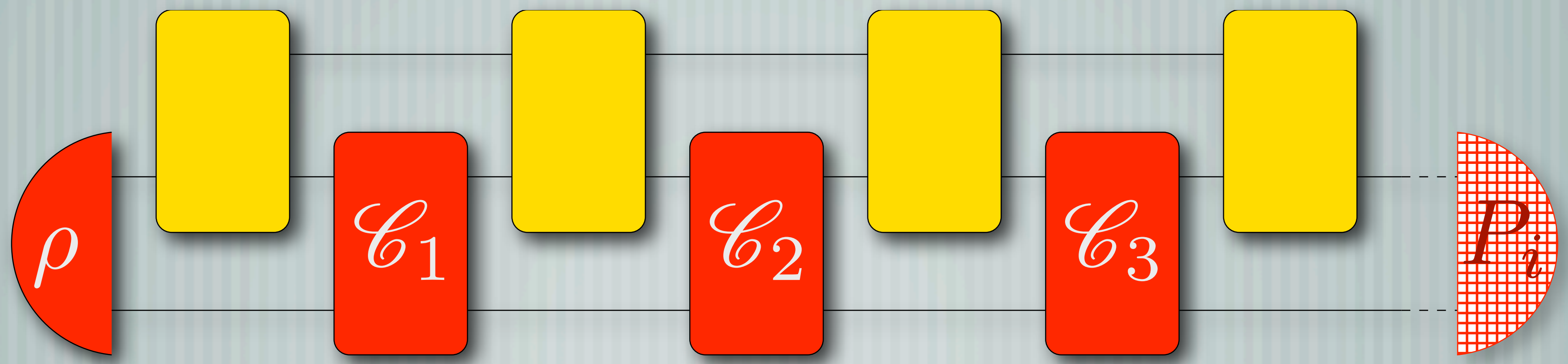
Decomposition of testers

A particularly useful decomposition for testers is

$$P_i := (I \otimes \Xi^{-\frac{1}{2}}) T_i (I \otimes \Xi^{-\frac{1}{2}})$$

$$\tilde{R} := (I \otimes \Xi^{T\frac{1}{2}}) R (I \otimes \Xi^{T\frac{1}{2}})$$

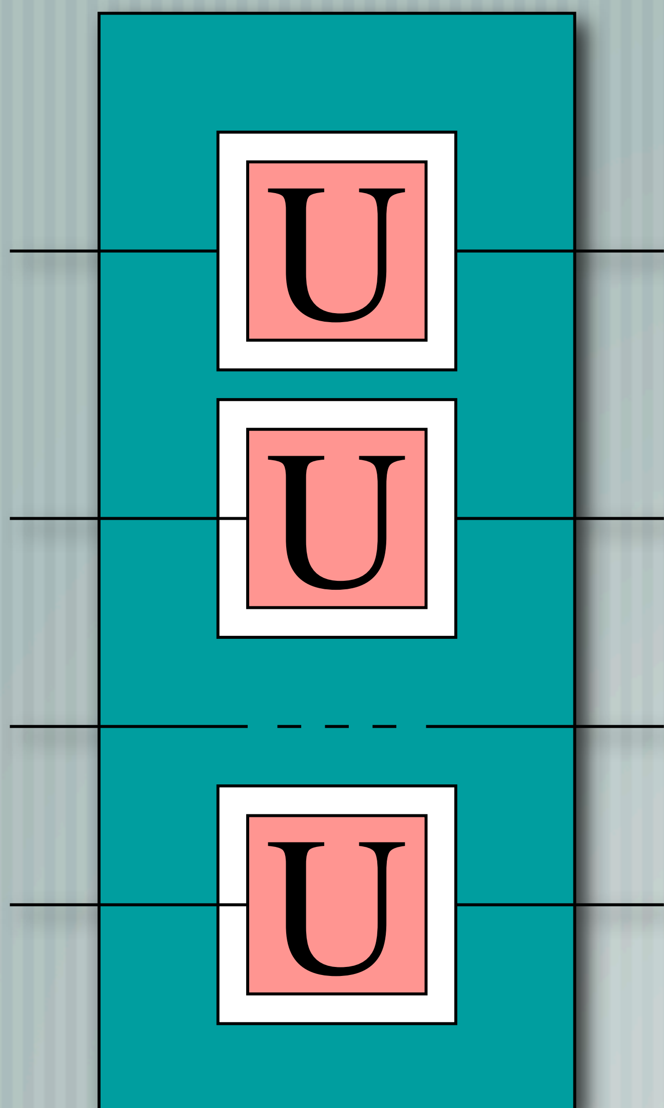
$$\mathrm{Tr}[R T_i^T] = \mathrm{Tr}[\tilde{R} P_i^T]$$



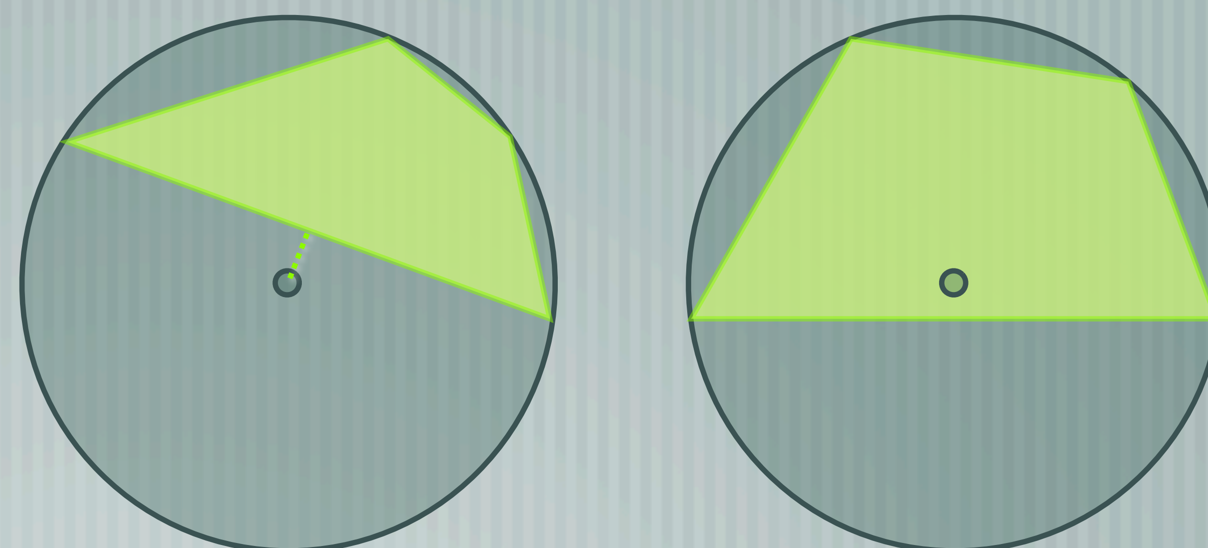
Discrimination of unitaries

- Problem: provided N uses of a black box which performs either U_1 or U_2, discriminate the two cases
- Procedure 1: apply the N uses on a multipartite state and measure
- Procedure 2: apply the N uses in sequence on a single system, intercalated with fixed unitaries, and measure
- Procedure 3: insert the N uses in a quantum network and measure the output

Procedure 1



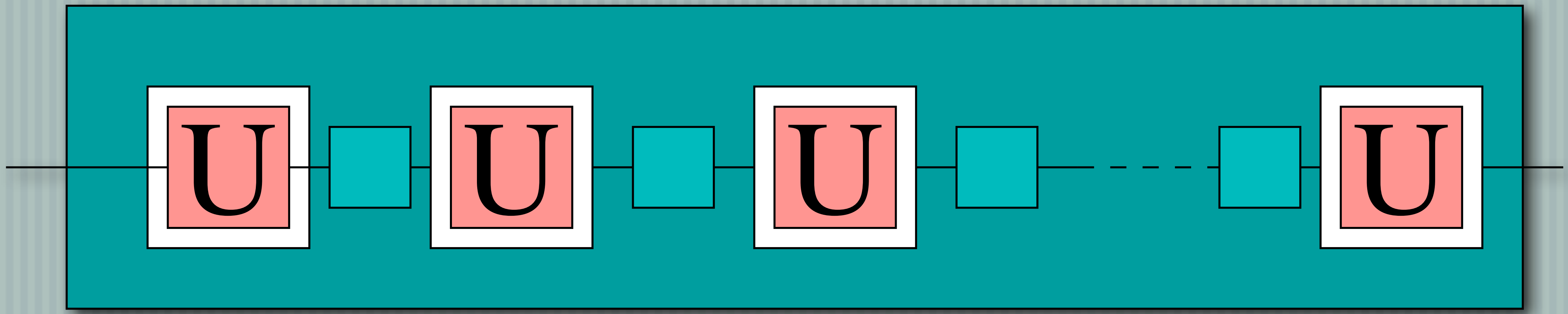
$$V = U_1^\dagger U_2$$



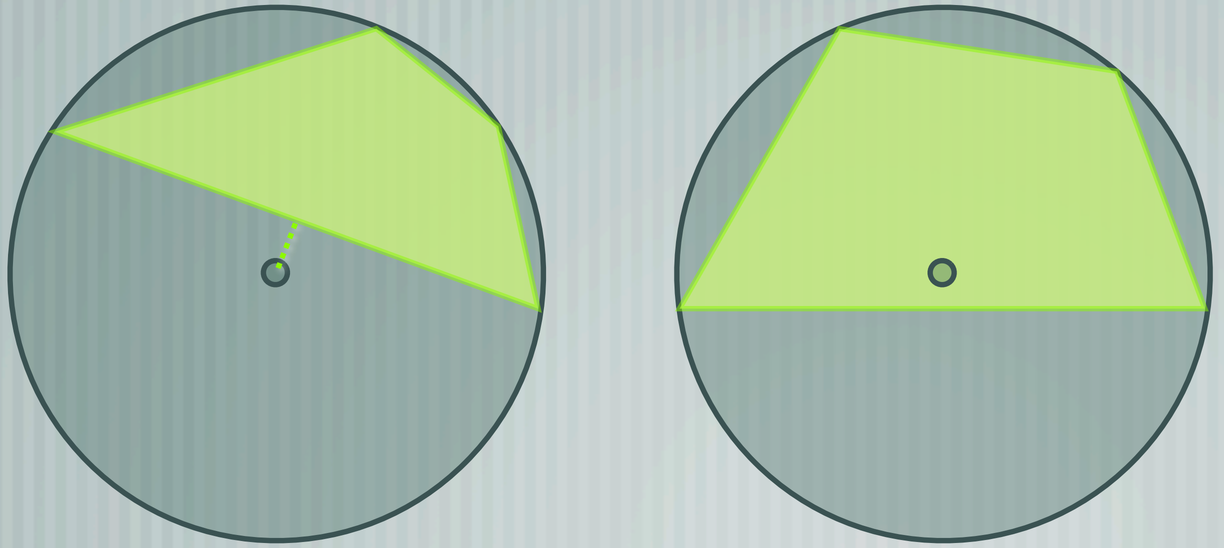
$$N_1 = \left\lceil \frac{\pi}{\Delta\phi} \right\rceil$$

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

Procedure 2



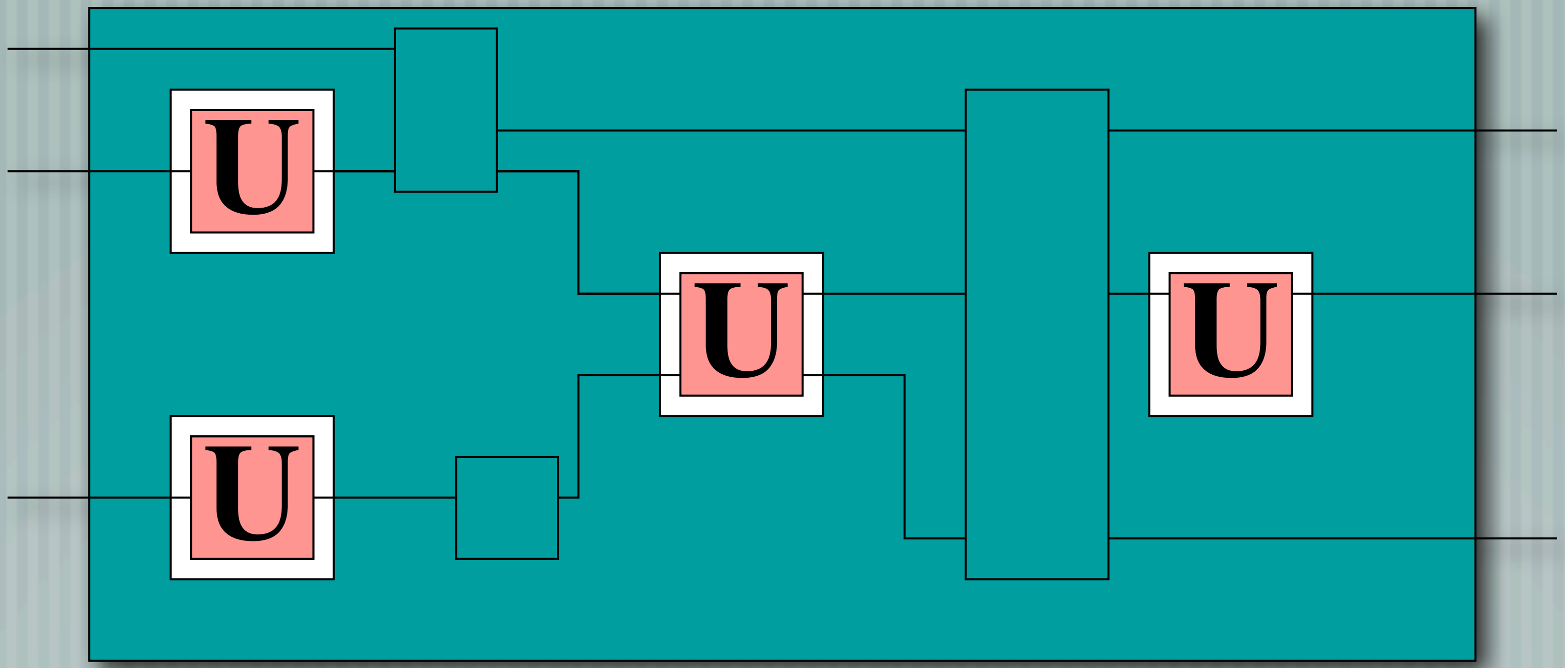
$$V = U_1^\dagger U_2$$



$$N_2 = N_1 = \left\lceil \frac{\pi}{\Delta\phi} \right\rceil$$

R. Duan, Y. Feng, M. Ying, PRL 98, 100503 (2007)

Procedure 3



Question: what is the optimal disposition of unitaries for discrimination?

Spread lemma

$\Delta(AB) \leq \Delta(A) + \Delta(B)$ A. M. Childs, J. Preskill, and J. Renes, J. Mod. Opt. 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 and fully sequential scheme are both optimal

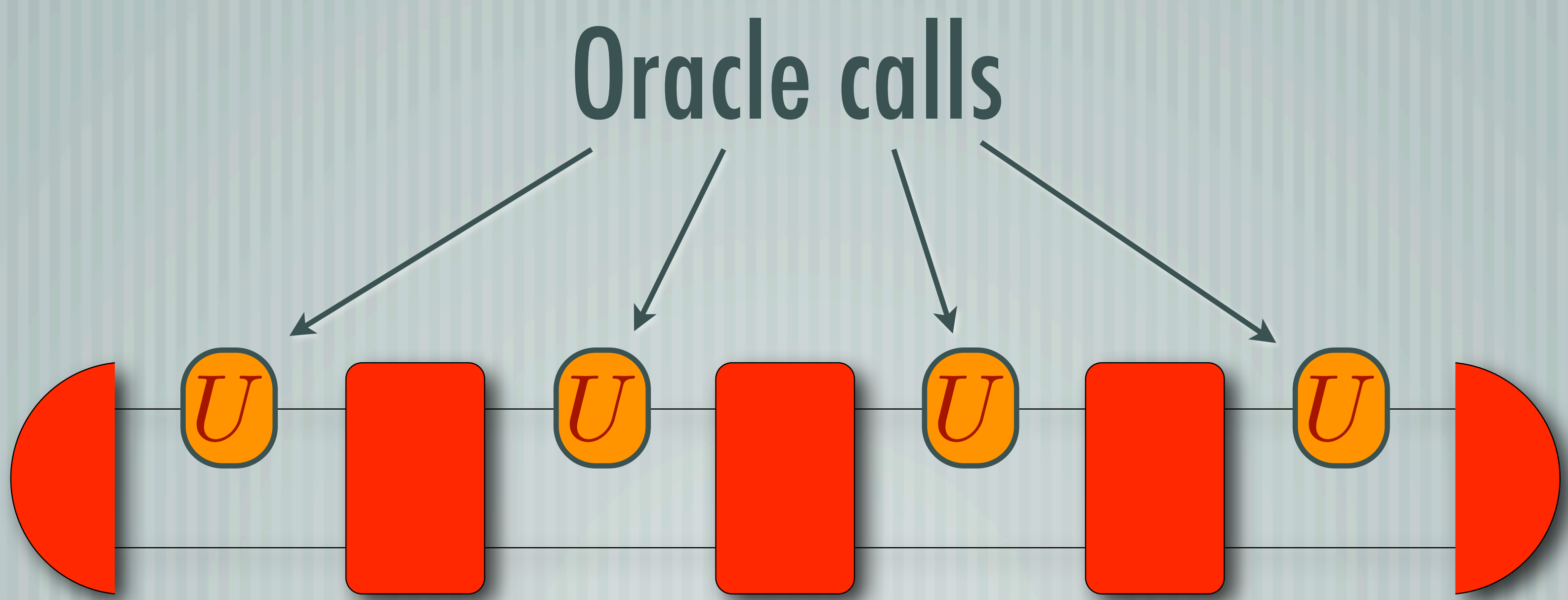
No quantum memory or entanglement are required

For optimal unambiguous discrimination only the POVM is different

G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 180501 (2008).

Discrimination of unitaries

- What happens for more than two unitaries?
- What happens for discrimination between sets of unitaries?
  - Quantum computation (e.g. Grover, Deutsh-Jozsa, Simon)



In general quantum memory is required

C. Zalka, Phys. Rev. A 60, 2746 (1999)

Conditions for discrimination

- Discriminability of multiple use channels and more generally combs is determined by optimized testers
  - What are conditions for perfect discriminability?
  - Is optimal discrimination parallel?

★ perfect discriminability $C_0(I_{2N-1} \otimes \Xi)C_1 = 0$

equivalently $|(I \otimes \sqrt{\Xi})(\sqrt{C_0} + \lambda\sqrt{C_1})|^2 \geq |(I \otimes \sqrt{\Xi})\sqrt{C_0}|^2, \quad \forall \lambda \in \mathbb{C}$

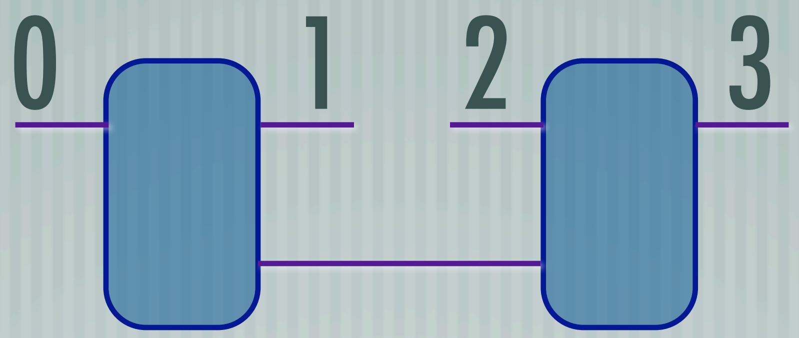
$$|X| := \sqrt{X^\dagger X}$$

G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 180501 (2008).

Sequential discrimination

★ optimal discriminability for combs is not parallel

Example:



$$C_0 = \sum_{p,q=0}^{d-1} |W^{\dagger}_{p,q}\rangle\rangle\langle\langle W^{\dagger}_{p,q}|_{3,2} \otimes \frac{|p,q\rangle\langle p,q|_1}{d^2} \otimes I_0,$$

$$C_1 = |0\rangle\langle 0|_3 \otimes I_2 \otimes \frac{I_1}{d^2} \otimes I_0$$

Operational network distance

Existence of non parallel optimal discrimination schemes

$\Downarrow$

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

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

$$\Delta := C - D$$

CB-norm distance only accounts for parallel discrimination schemes

G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 180501 (2008).

Covariant estimation of unitaries

- Covariant unitary estimation problem:
  - A group of unitaries, (Haar-distributed) $|U_g\rangle\!\rangle\langle\!\langle U_g|$
  - A general tester for estimating the group element T_h
  - What is the optimal tester?
- One can prove that the optimal tester is covariant

$$T = \int_G \mathrm{d}\, g T_g$$

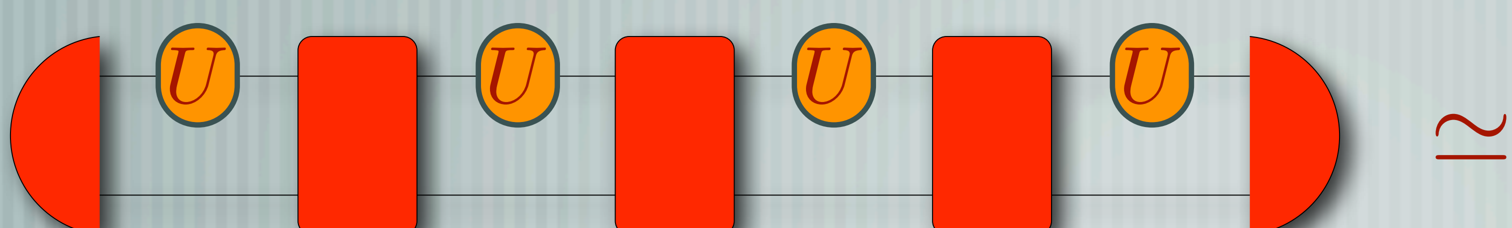
$$T_h = (U_h^{\otimes N} \otimes I)\Theta(U_h^{\dagger\otimes N} \otimes I) \quad \Rightarrow \quad [T, U_h^{\otimes N} \otimes I] = 0$$

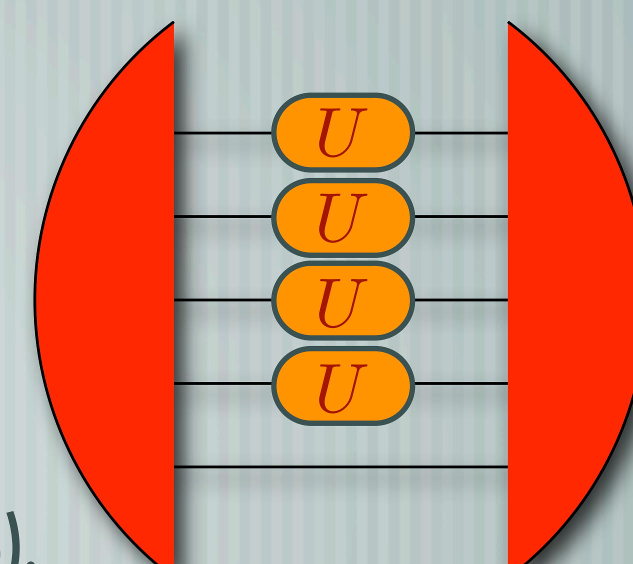
Parallelization

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

Any covariant tester prepares a set of covariant states

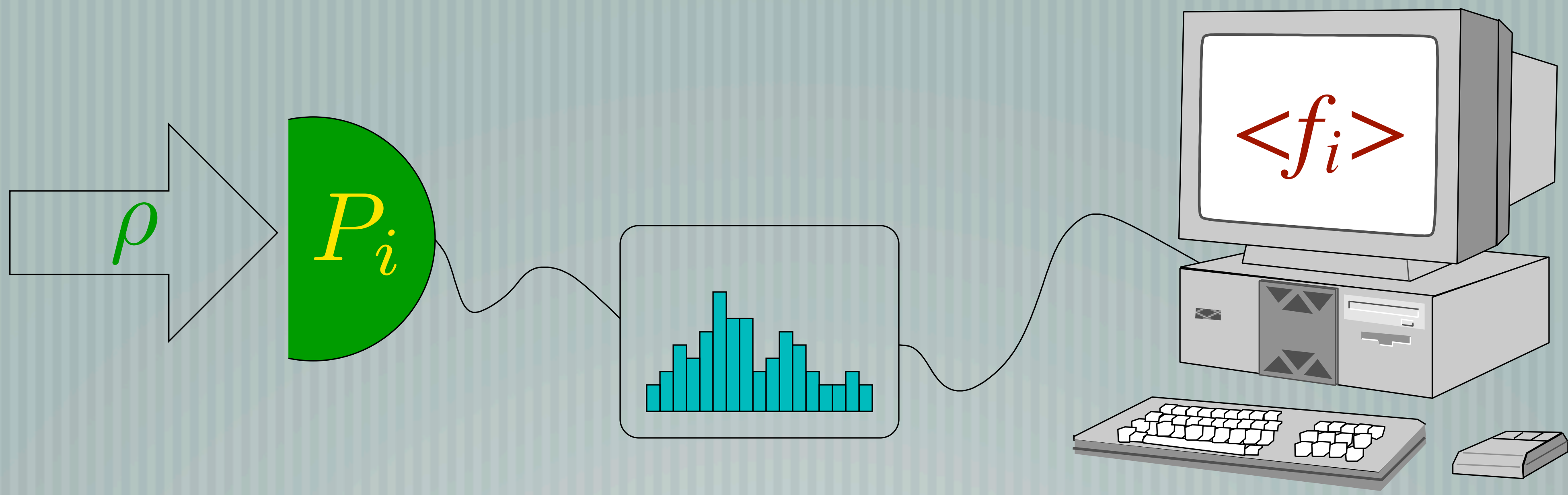
Any covariant tester is equivalent to a parallel scheme





G. Chiribella, G. M. D'Ariano, and P. P., Phys. Rev. Lett. 101, 180501 (2008).

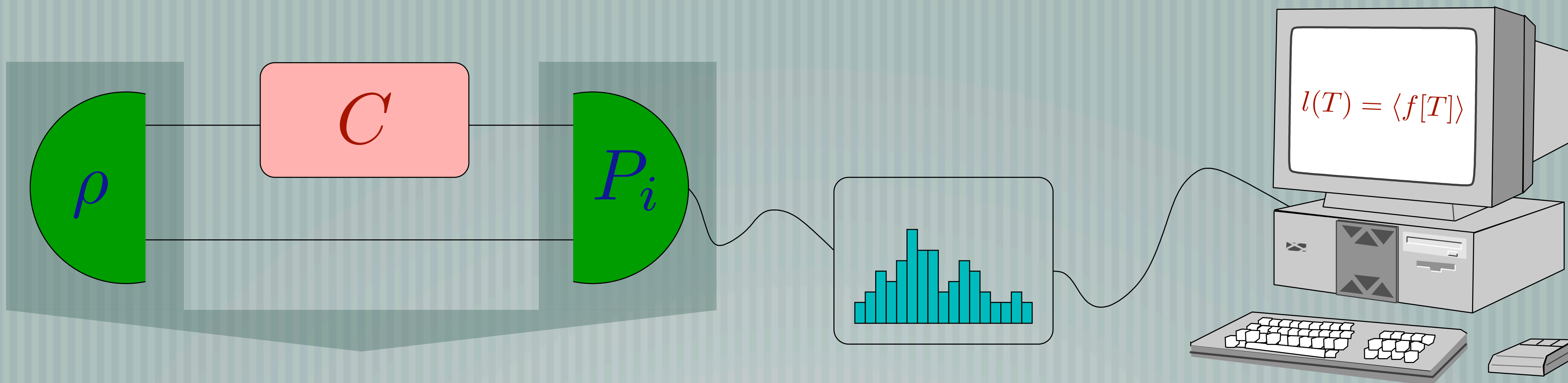
Tomography



$$\langle O \rangle = \sum_i f_i(O)\, \mathrm{Tr}[P_i \rho]$$

The POVM must be informationally complete

Process tomography



Tester T_i

$$\mathrm{Tr}[CX] = \sum_i f_i[X]\,\mathrm{Tr}[T_i C]$$

The tester must be informationally complete

Optimization

- Tomogrphy - reconstruction of linear parameters
- Problem: how to achieve the minimum statistical error?
- In both cases f_i is generally not unique
  - What is the best processing for a fixed POVM/tester?
- Comparing POVMs/testers with optimal processing
  - What is the optimal POVM/tester?

Optimal processing

$$P_i \to \Lambda : \quad \Lambda c = \sum_i c_i P_i$$

$$f[X] = \Gamma(X), \quad \Lambda\Gamma\Lambda = \Lambda$$

Statistical error:

$$\Delta(X) := \sum_i |f_i[X]|^2 \, \mathrm{Tr}[P_i \rho_{\mathcal{E}}] - \overline{|\langle X \rangle|^2}_{\mathcal{E}}$$

$$\rho_{\mathcal{E}} := \int p_{\mathcal{E}}(\mathrm{d}\,\rho)\rho \qquad \overline{g(\rho)}_{\mathcal{E}} := \int p_{\mathcal{E}}(\mathrm{d}\,\rho) g(\rho)$$

Optimal processing

$$P_i \to \Lambda : \quad \Lambda c = \sum_i c_i P_i$$

$$f[X] = \Gamma(X), \quad \Lambda\Gamma\Lambda = \Lambda$$

Statistical error:

$$\Delta(X) := \sum_i |f_i[X]|^2 \operatorname{Tr}[P_i \rho_{\mathcal{E}}] - \overline{|\langle X \rangle|^2}_{\mathcal{E}}$$

$$\rho_{\mathcal{E}} := \int p_{\mathcal{E}}(\mathrm{d}\,\rho)\rho \qquad \overline{g(\rho)}_{\mathcal{E}} := \int p_{\mathcal{E}}(\mathrm{d}\,\rho) g(\rho)$$

Optimal processing

The only term depending on P_i and Γ can be written as a norm

$$\|f[X]\|_\pi^2 := \sum_i f_i^*[X]\pi_{ij} f_j[X]$$

The optimal f_i must satisfy $\pi\Gamma\Lambda = \Lambda^\dagger\Gamma^\dagger\pi$

Solution $\Gamma = \Lambda^\ddagger - [(I - \Lambda^\ddagger\Lambda)\pi(I - \Lambda^\ddagger\Lambda)]^\ddagger\pi\Lambda^\ddagger$

$$\pi_{ij} = \delta_{ij}\,\mathrm{Tr}[P_i\rho_{\mathcal{E}}]$$

G. M. D'Ariano and P. P., Phys. Rev. Lett. 98, 020403 (2007).

Optimal process tomography

$$\mathrm{Tr}[CX] = \sum_i f_i[X]\,\mathrm{Tr}[T_iC]$$

- Problem: minimum statistical error reconstruction
- The problem is formally the same as for states
  - the optimal processing can be found in the same way

Optimal tester

- Figure of merit: weighted sum of errors for a set of expectation values
- Assumption: the average channel/quantum operation of the ensemble is the totally depolarizing

$$C_{\mathcal{E}} := \int p(\mathrm{d}\, C) C = \frac{I}{d_{\mathrm{out}}}$$

In this case $\overline{g(C)}_{\mathcal{E}} := \int p_{\mathcal{E}}(\mathrm{d}\, C) g(C)$

Optimal tester

One can prove that the error in estimating $\mathrm{Tr}[CZ]$ is

$$\langle\langle Z|X^{-1}|Z\rangle\rangle - \overline{\mathrm{Tr}[RZ]^2}_{\mathcal{E}}$$

And for a set of operators the weighted sum is

$$\mathrm{Tr}[X^{-1}G], \quad G := \sum_i w_i |Z_i\rangle\rangle\langle\langle Z_i|$$

We considered $G = I$

A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. P., Phys. Rev. Lett. 102, 010404 (2009).

Optimal tester

One can prove that the error in estimating $\mathrm{Tr}[CZ]$ is

$$\langle\langle Z|X^{-1}|Z\rangle\rangle - \overline{\mathrm{Tr}[RZ]^2}_{\mathcal{E}}$$

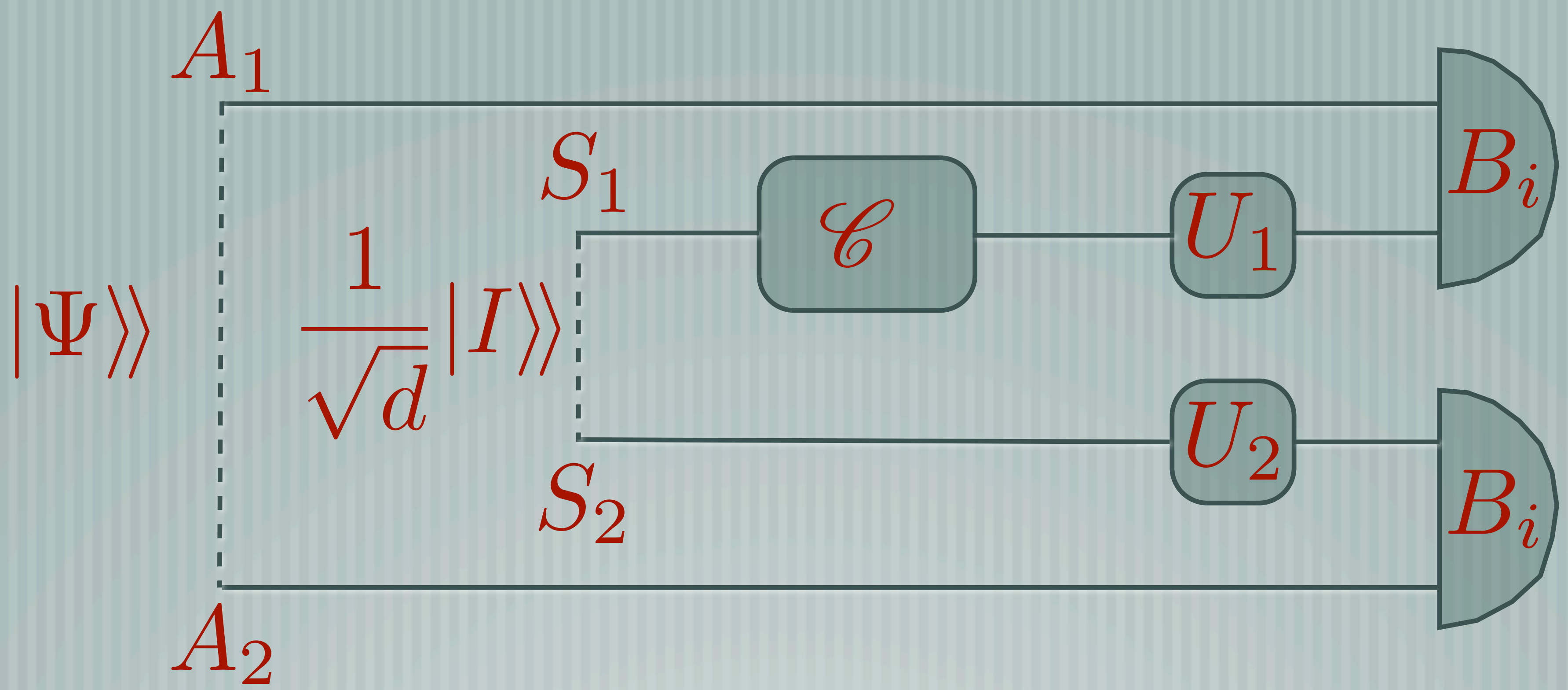
And for a set of operators the weighted sum is

$$\mathrm{Tr}[X^{-1}G], \quad G := \sum_i w_i |Z_i\rangle\rangle\langle\langle Z_i|$$

We considered $G = I$

A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. P., Phys. Rev. Lett. 102, 010404 (2009).

Optimal tester

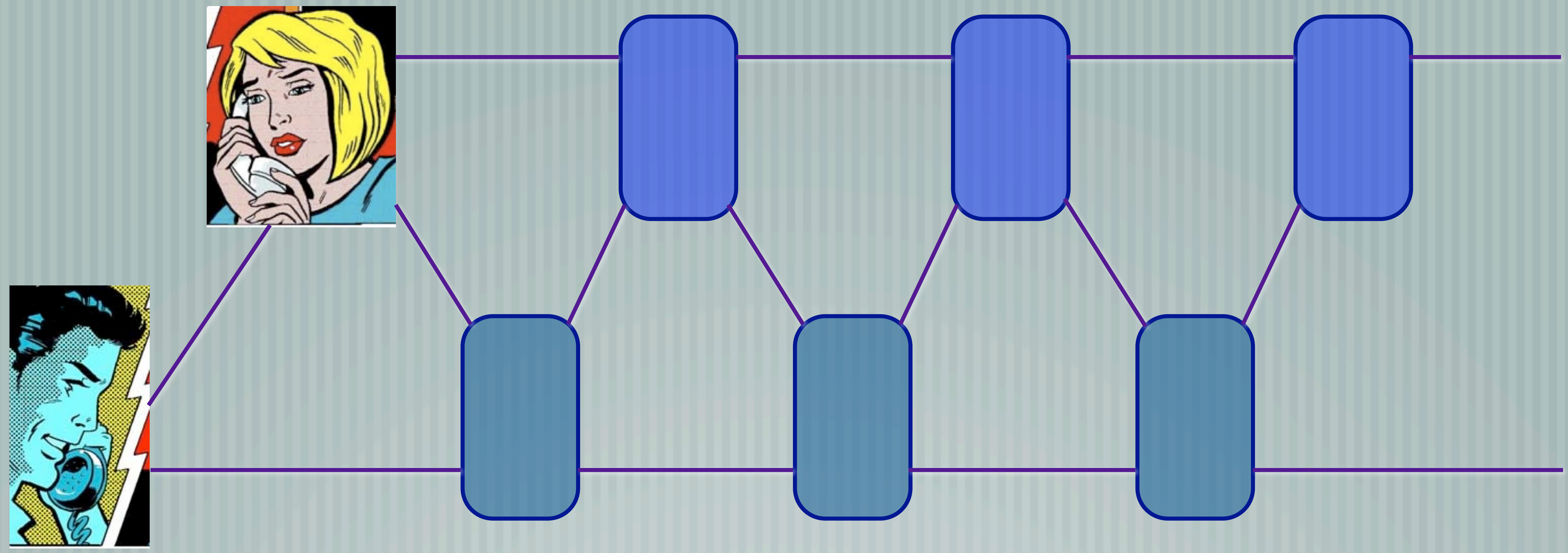


The choice of Ψ depends on the set we want to tomograph

e.g. channels, quantum operations, states, POVMs

A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. P., Phys. Rev. Lett. 102, 010404 (2009).

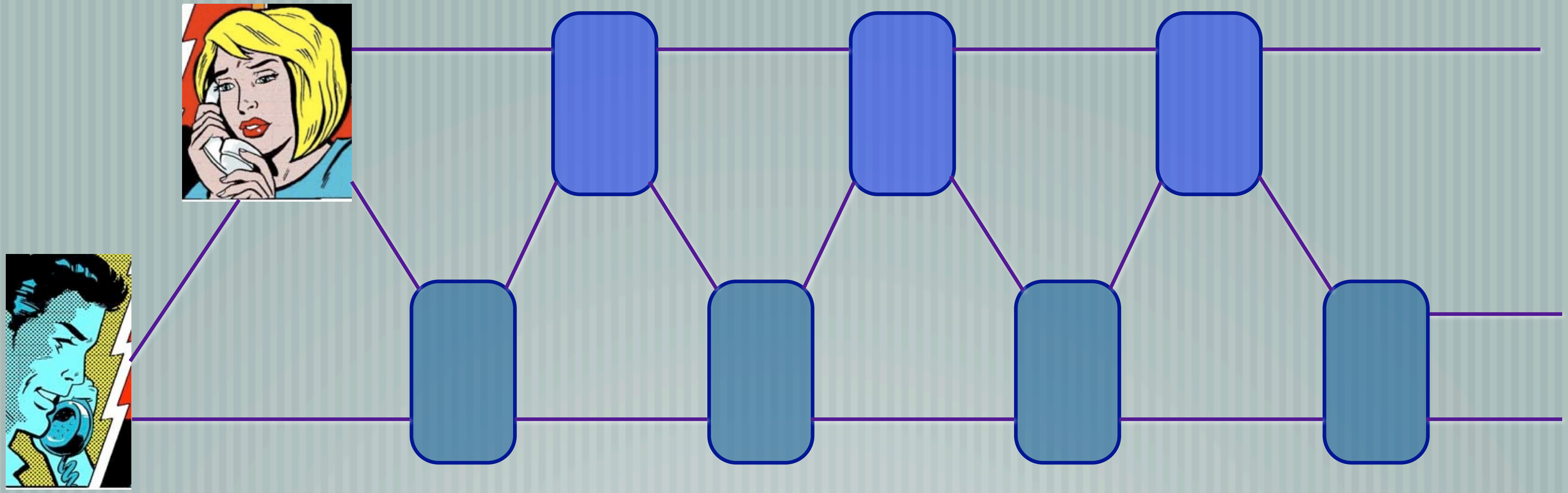
Quantum protocols



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

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

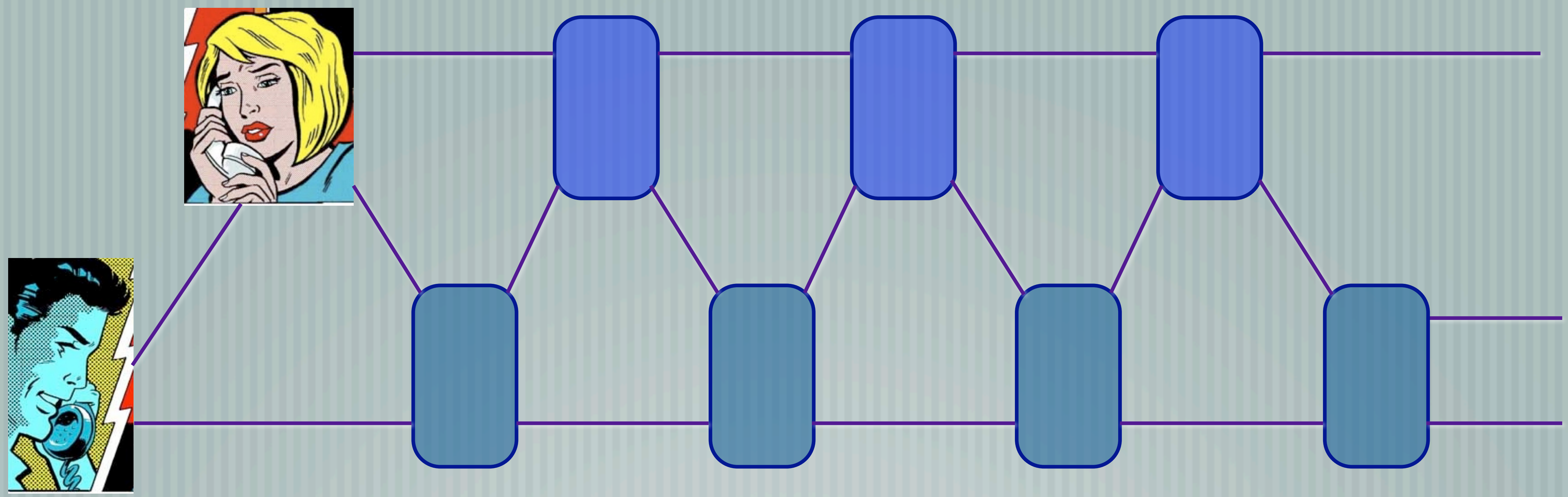
Bit commitment



Quantum combs can describe the most general strategies in a quantum bit commitment protocol

The protocol must be: binding and concealing

Sketch of impossibility proof



- Alice has two strategies with small operational distance (binding)
- Then, by a transformation on her ancilla Alice can move from 0 to another comb which has small operational distance from 1(not concealing)

G. Chiribella, G. M. D'Ariano, P. P., D. Schlingemann, and R. F. Werner, in preparation.

Concluding remarks

- The theory of combs allows to account for complex situations (networks) by simple tools (positive operators)
- The applications show a wide range of problems that can be solved through the theory of combs and testers
- We would like in the future to study the foundational aspects of combs
- G. Chiribella, G. M. D'Ariano, and P. P., in preparation

Thank you

for your attention

More information at www.qubit.it