Title: Self-Testing of Quantum Circuits

Date: Nov 15, 2006 02:00 PM

URL: http://pirsa.org/06110011

Abstract: I will explain how a quantum circuit together with measurement apparatuses and EPR sources can be fully verified without any reference to some other trusted set of quantum devices. Our main assumption is that the physical system we are working with consists of several identifiable sub-systems, on which we can apply some given gates locally.
To achieve our goal we define the notions of simulation and equivalence. The concept of simulation refers to producing the correct probabilities when measuring physical systems. The notion of equivalence is used to enable the efficient testing of the composition of quantum operations. Unlike simulation, which refers to measured quantities (i.e., probabilities of outcomes), equivalence relates mathematical objects like states, subspaces or gates.
Using these two concepts, we prove that if a system satisfies some simulation conditions, then it is equivalent to the one it is supposed to implement. In addition, with our formalism, we can show that these statements are robust, and the degree of robustness can be made explicit. Finally, we design a test for any quantum circuit whose complexity is linear in the number of gates and qubits, and polynomial in the required precision.
Joint work with Frederic Magniez, Dominic Mayers and Harold Ollivier.

University of Waterloo

IQC Institute for Quantum Computing

Self-Testing of Quantum Circuits

Michele Mosca

Canada Research Chair in Quantum Computation

Joint with F. Magniez, D. Mayers, H. Ollivier

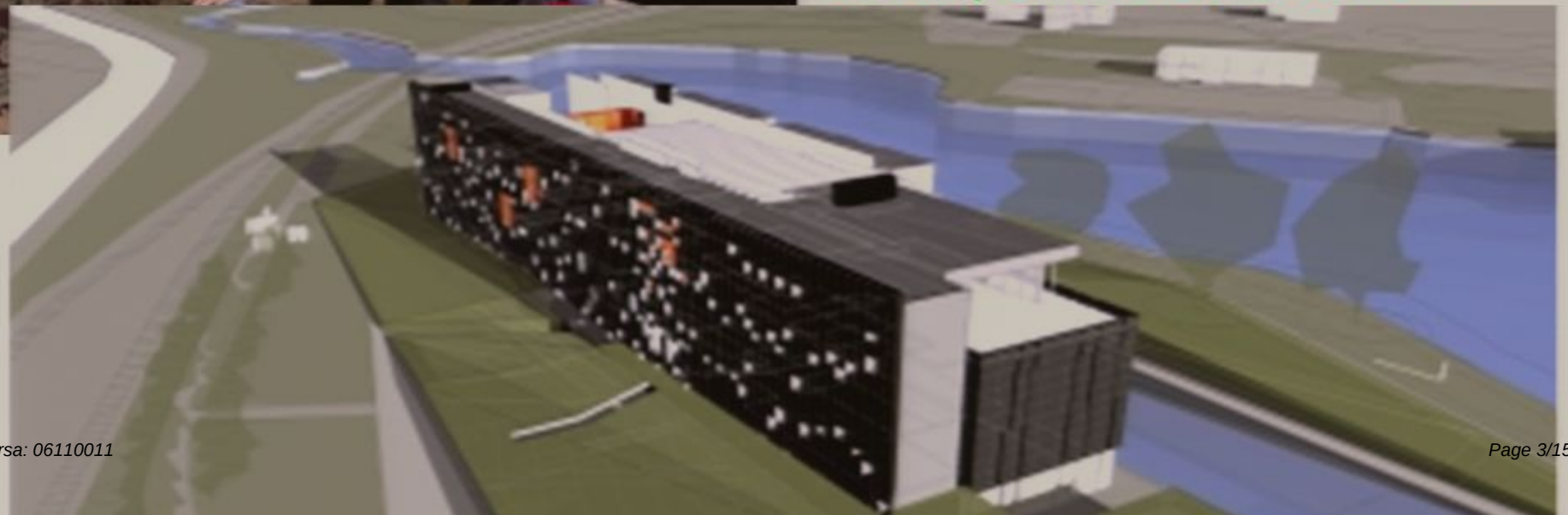
Perimeter Institute Colloquium

15 November 2006

PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

Perimeter Institute is a community of theoretical physicists dedicated to investigating fundamental issues in theoretical physics.

www.perimeterinstitute.ca



IQC Institute for Quantum Computing

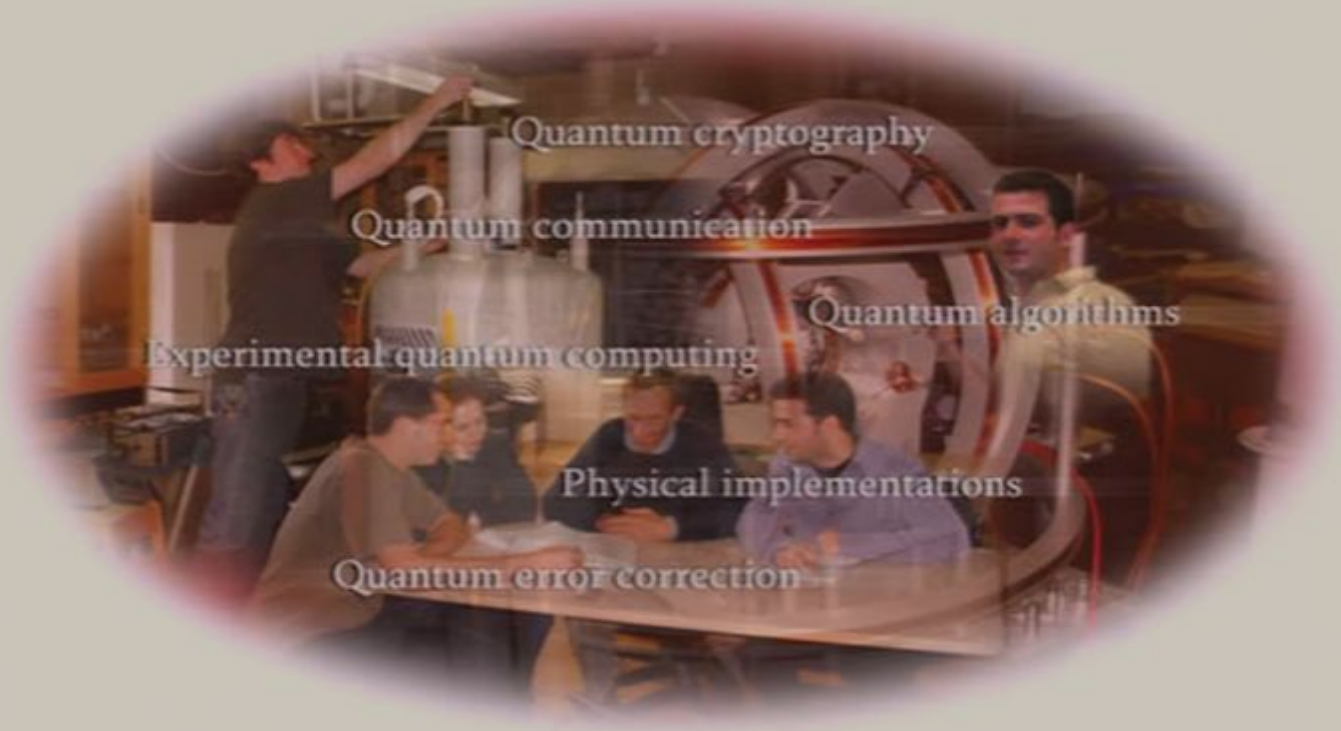
Centre for Applied Cryptographic Research

The University of Waterloo

SJU

IN SANCTITATE ET IUSTITIA

SPLENDESCIT ARDOR LABORIS



www.iqc.ca

Outline

Outline

Why do we want to test?

Outline

Why do we want to test?

What did we already know?

Outline

Why do we want to test?

What did we already know?

Current status.

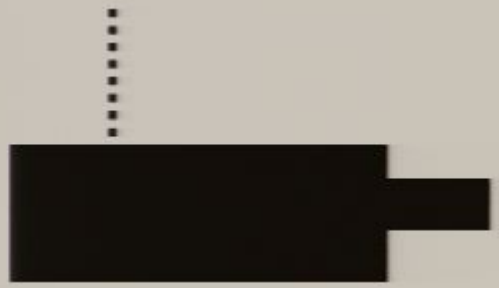
Why do we want to test?

Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

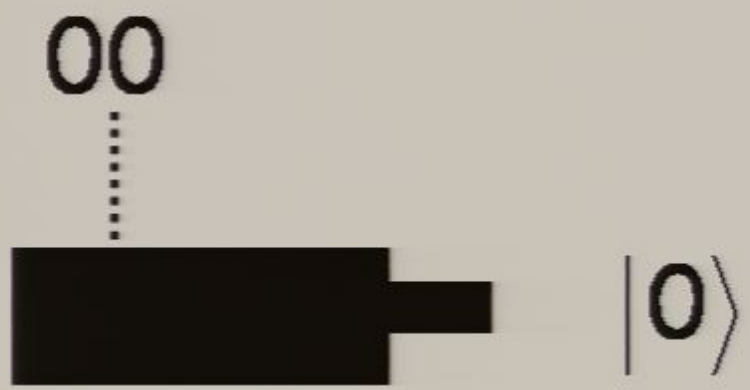
Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

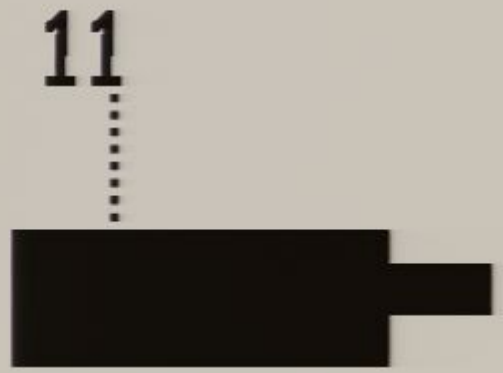
Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.



$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

Why should you trust this component?

Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

Why should you trust this component?

Why not?

Why do we want to test?

Suppose you wish to buy a component for BB84 quantum cryptography, e.g. a source.

Why should you trust this component?

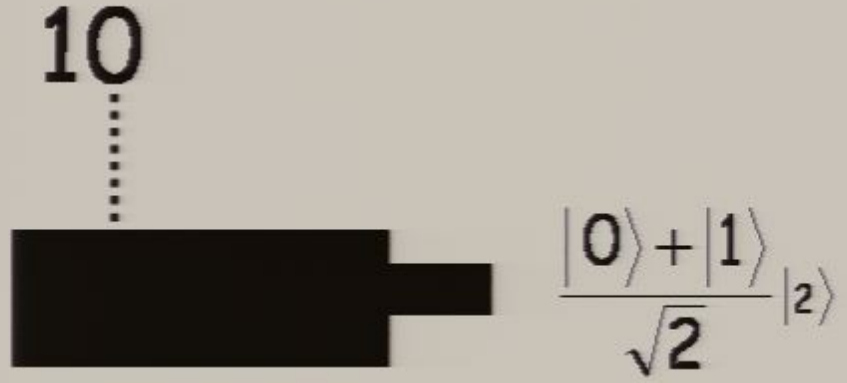
Why not?
What if what we really have is implementing the following?

Why not?
What if what we really have is implementing the following?

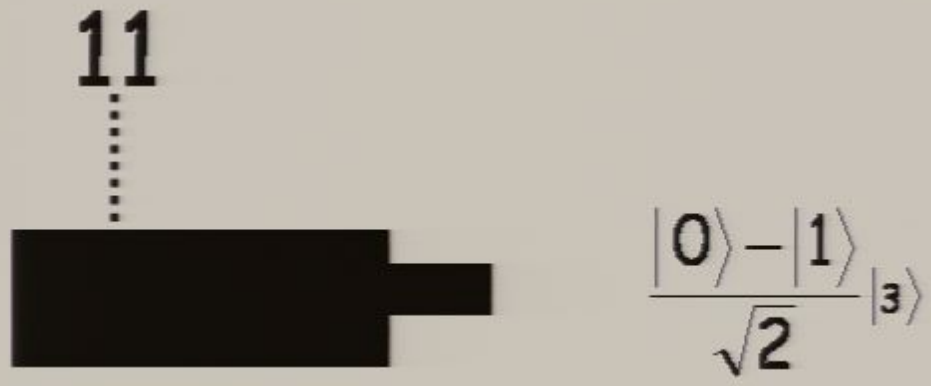
Why not?
What if what we really have is implementing the following?

Why not?
What if what we really have is implementing the following?

Why not?
What if what we really have is implementing the following?



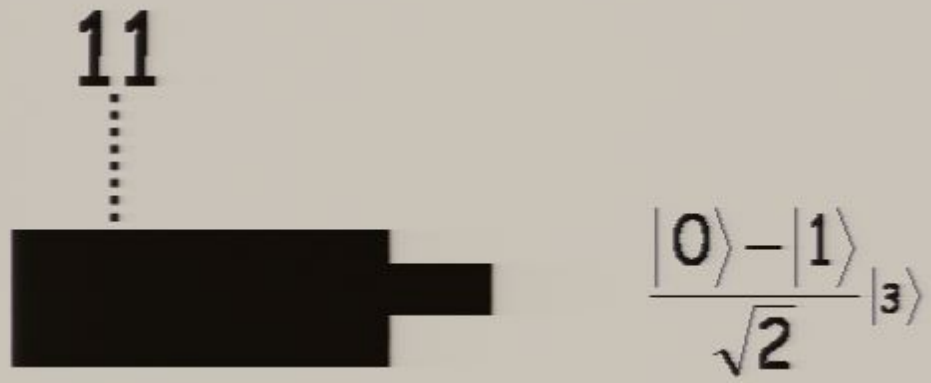
Why not?
What if what we really have is implementing the following?



Why not?
What if what we really have is implementing the following?

"side-channels"

Why not?
What if what we really have is implementing the following?



Why not?
What if what we really have is implementing the following?

"side-channels"

http://www.research.ibm.com/journal/rd/481/smolin.html

C. H. Bennett, F. Bessett, G. Brassard, L. Salvail, and J. Smolin, " Experimental Quantum Cryptography," J. Cryptol. 5, No. 1, 3–28 (1992).

Why not?
What if what we really have is impl
the following?

"side-channel

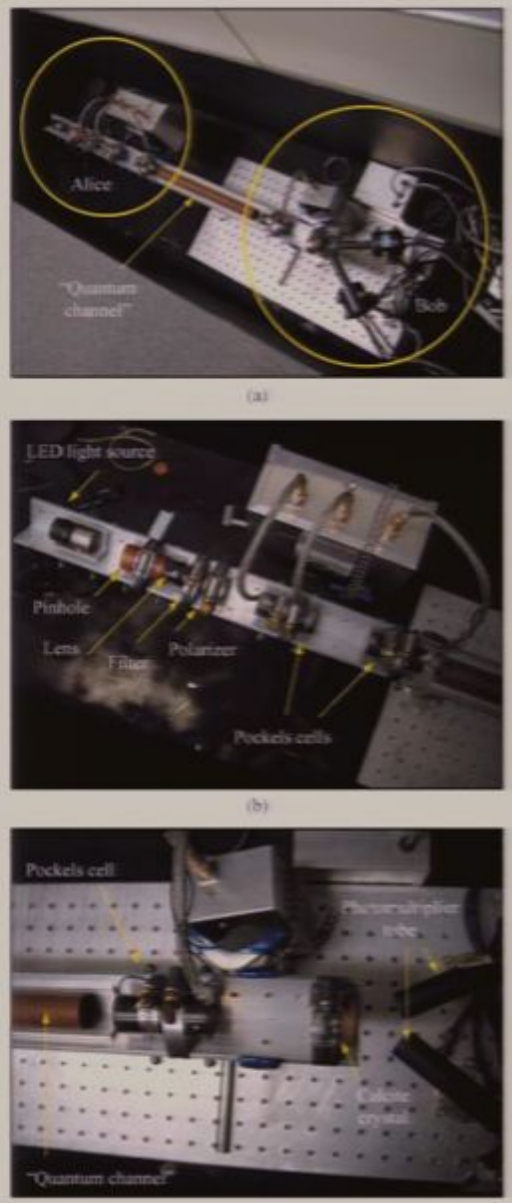


Figure 1

The apparatus used to perform the [illegible] cryptography experiment: (a) The entire apparatus; (b) detailed view of Alice; (c) detailed view of Bob.

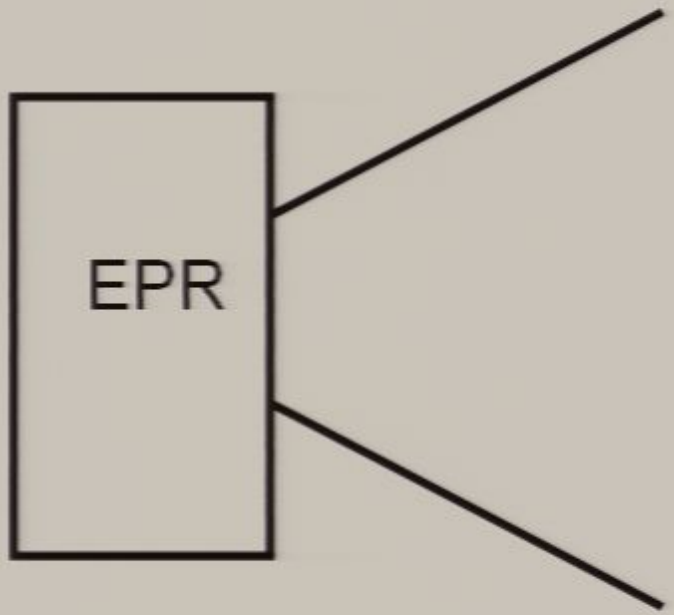
We need to make our assumptions and testing procedures explicit.

We need to make our assumptions and testing procedures explicit.

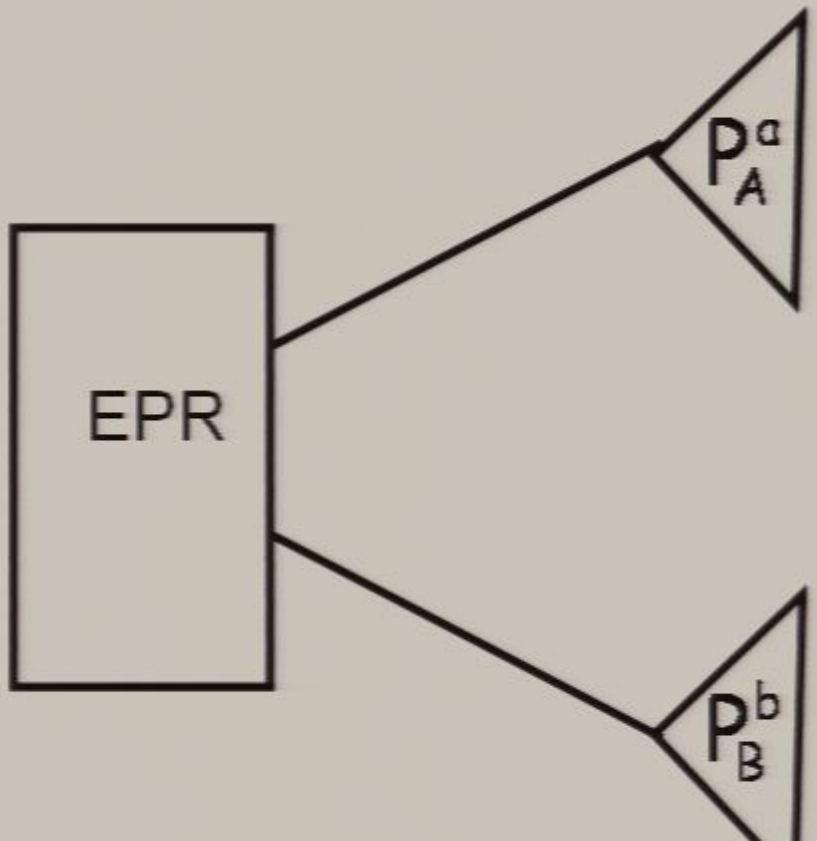
We also don't want to rely on some other untrusted apparatus (e.g. in order to "just" do tomography).

Mayers and Yao devised a scheme for "self"-testing ***sources*** *for the purposes of QKD.*

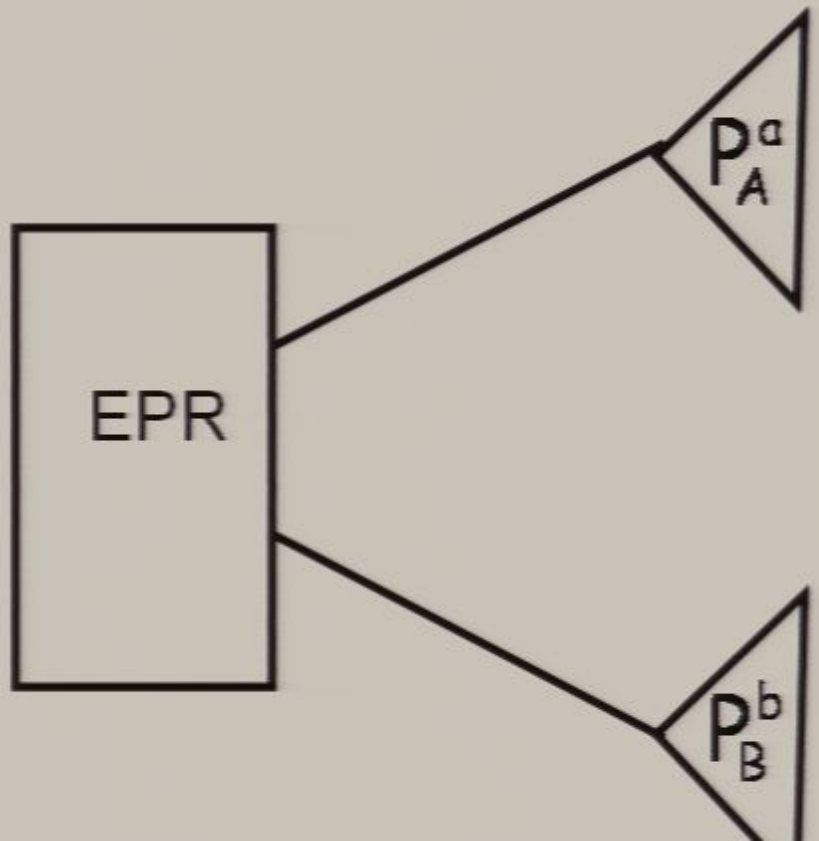
Mayers and Yao devised a scheme for "self"-testing ***sources*** *for the purposes of QKD.*



Mayers and Yao devised a scheme for "self"-testing ***sources*** *for the purposes of QKD.*



Mayers and Yao devised a scheme for "self"-testing ***sources*** *for the purposes of QKD.*



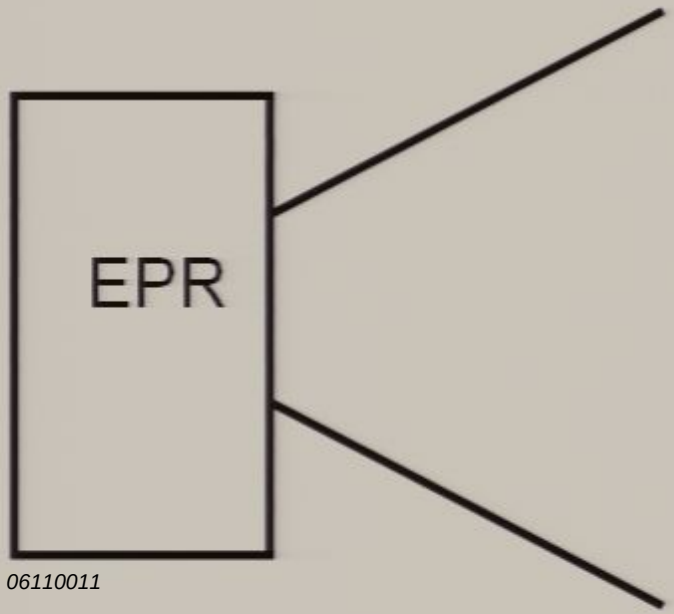
$$P^0 + P^{\pi/2} = I$$

$$P^{\pi/8} + P^{5\pi/8} = I$$

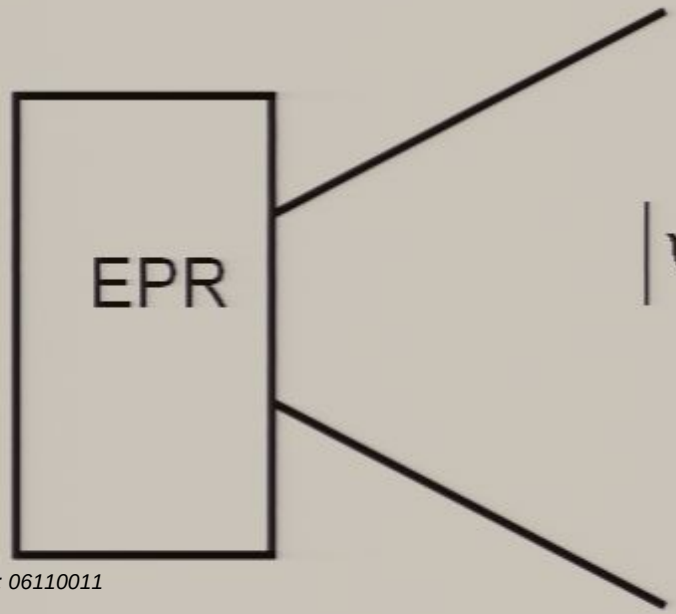
$$P^{\pi/4} + P^{3\pi/4} = I$$

If the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ *then the output of the sources is locally unitarily equivalent to a state containing* $|\varphi\rangle$ *, and the projections are consistent with measuring the EPR pair.*

If the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ *then the output of the sources is locally unitarily equivalent to a state containing* $|\varphi\rangle$ *, and the projections are consistent with measuring the EPR pair.*



If the statistics are consistent with $|\varphi\rangle = |00\rangle + |11\rangle$ *then the output of the sources is locally unitarily equivalent to a state containing* $|\varphi\rangle$, *and the projections are consistent with measuring the EPR pair.*



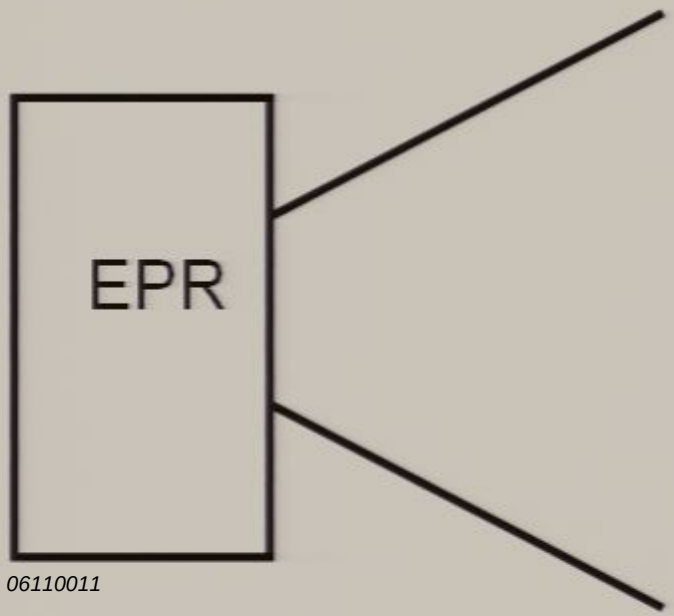
$$|\psi\rangle_{AB}$$

$$|\psi\rangle_{AB} = U_A \otimes U_B \left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB} \right)$$

Application of this result

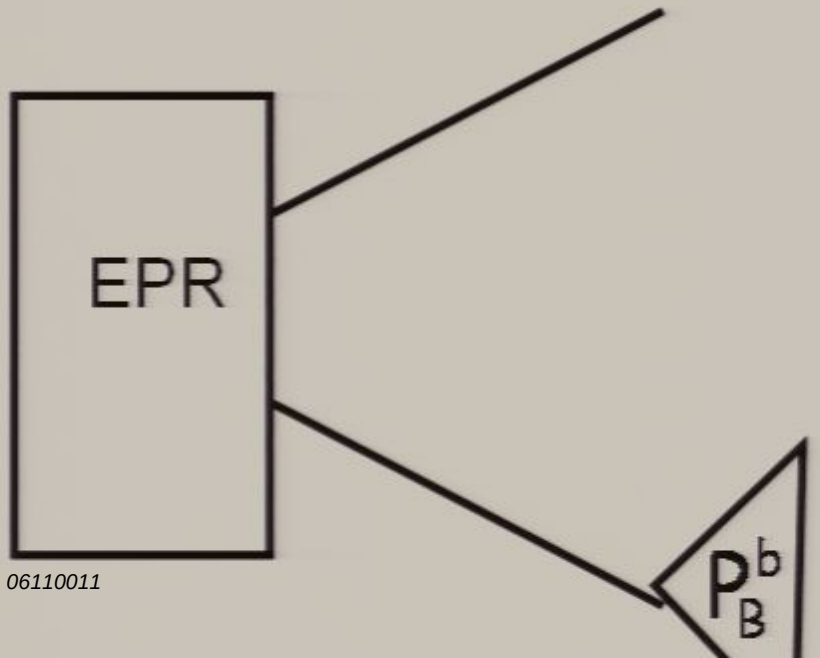
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B \left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB} \right)$$



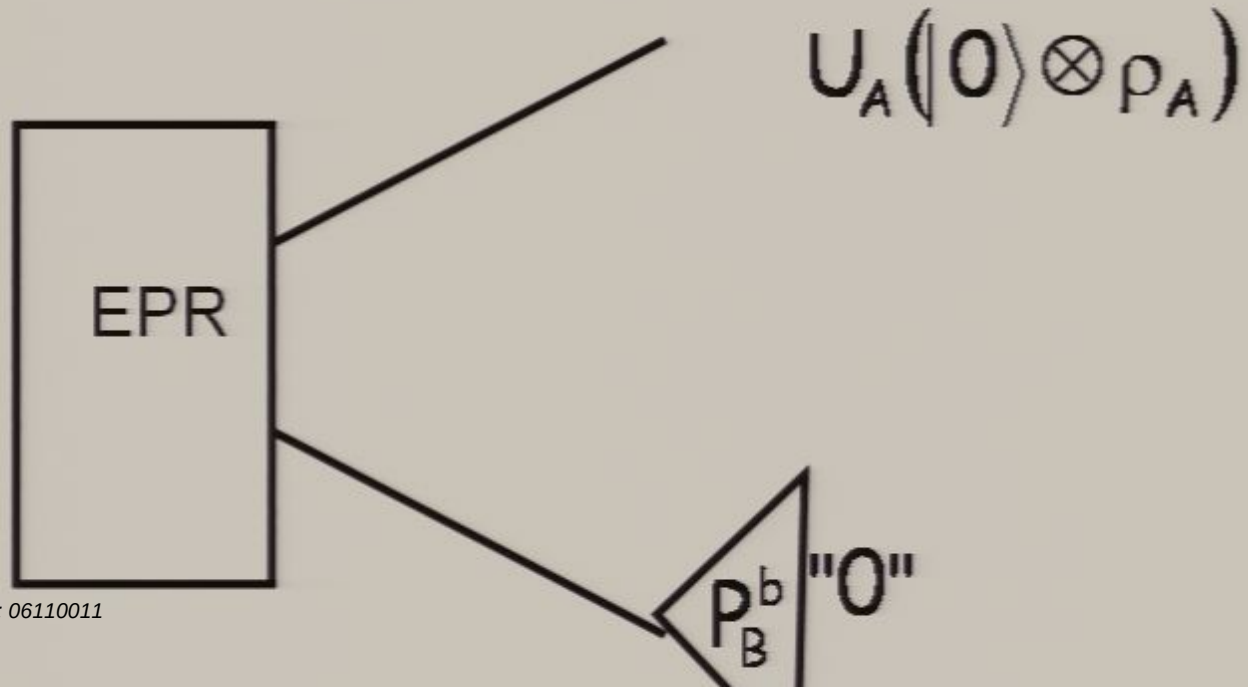
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



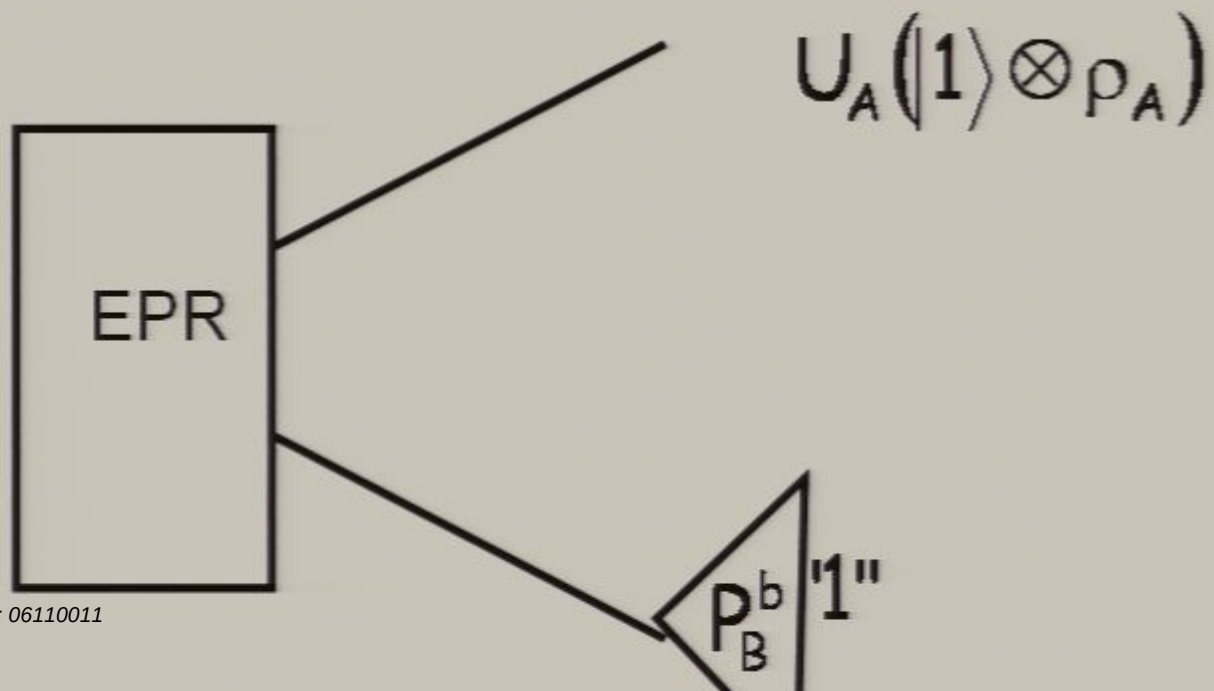
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



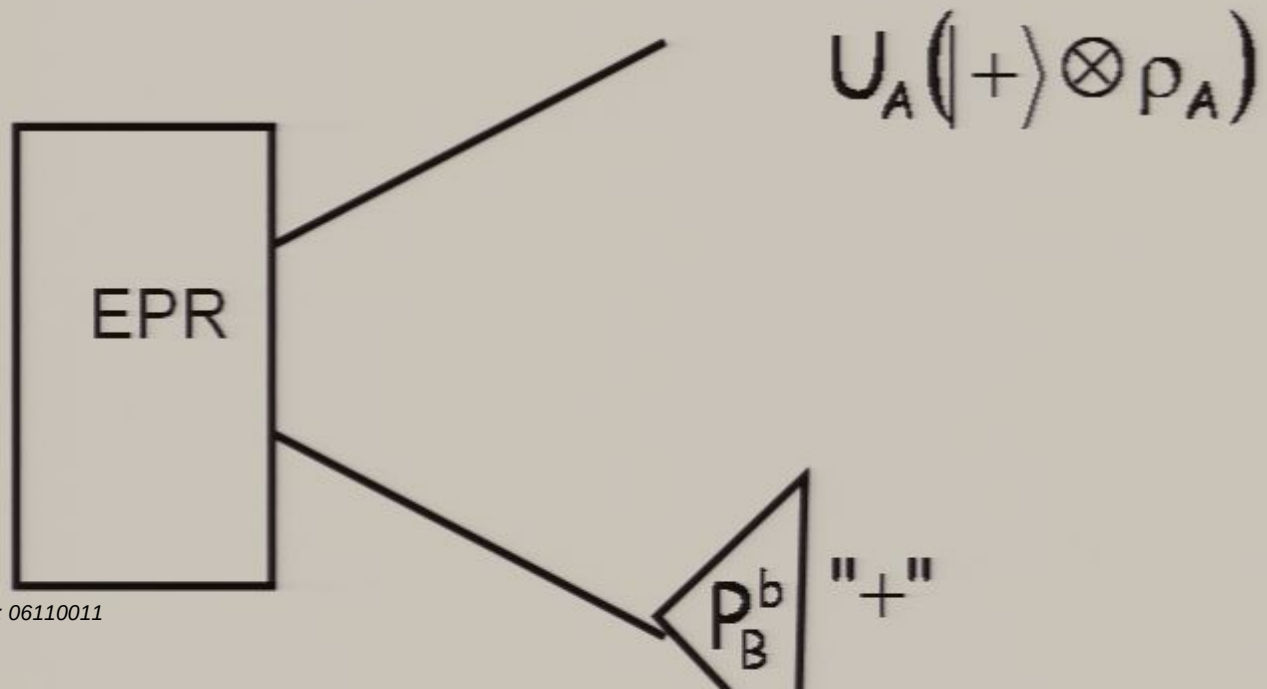
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



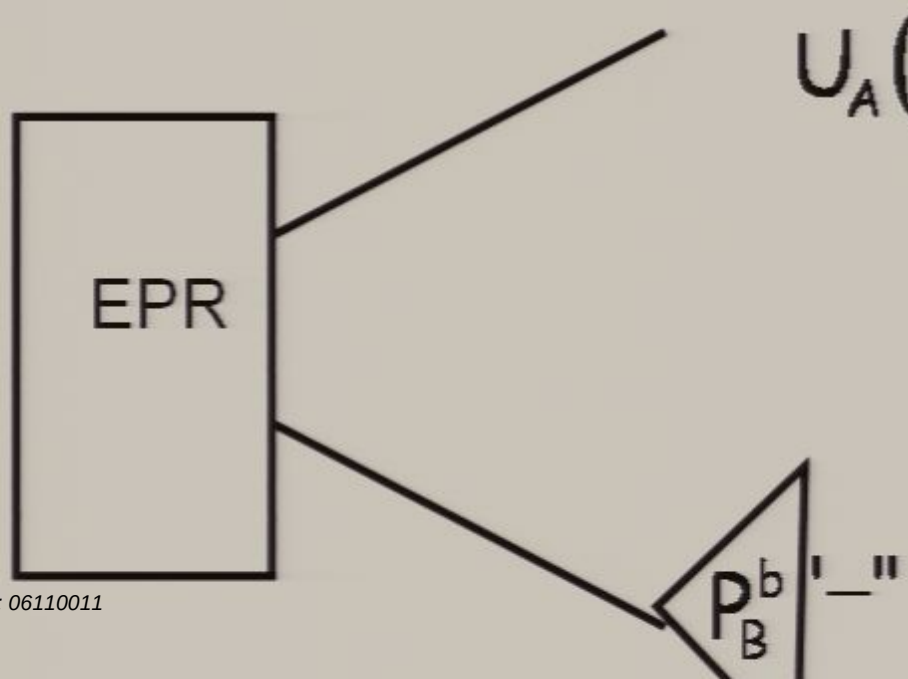
Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



Application of this result

$$|\psi\rangle_{AB} = U_A \otimes U_B\left(|\varphi\rangle_{AB} \otimes |\chi\rangle_{AB}\right)$$



The main assumptions of Mayers and Yao are

1) *Locality (i.e. measurements at A commute with those at B)*
2) *Repeatability of experiments*
3) *Trusted classical apparatus*

The main assumptions of Mayers and Yao are

1) *Locality (i.e. measurements at A commute with those at B)*
2) *Repeatability of experiments*
3) *Trusted classical apparatus*

However, the results are not "robust". The results hold exactly if the statistics are satisfied exactly.

Any realistic application will need to be robust.

The main assumptions of Mayers and Yao are

1) *Locality (i.e. measurements at A commute with those at B)*
2) *Repeatability of experiments*
3) *Trusted classical apparatus*

However, the results are not "robust". The results hold exactly if the statistics are satisfied exactly.

Any realistic application will need to be robust.

(Assuming robustness) This might be the only way, using only these assumptions, to verifiably securely

Why else do we want to test?

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

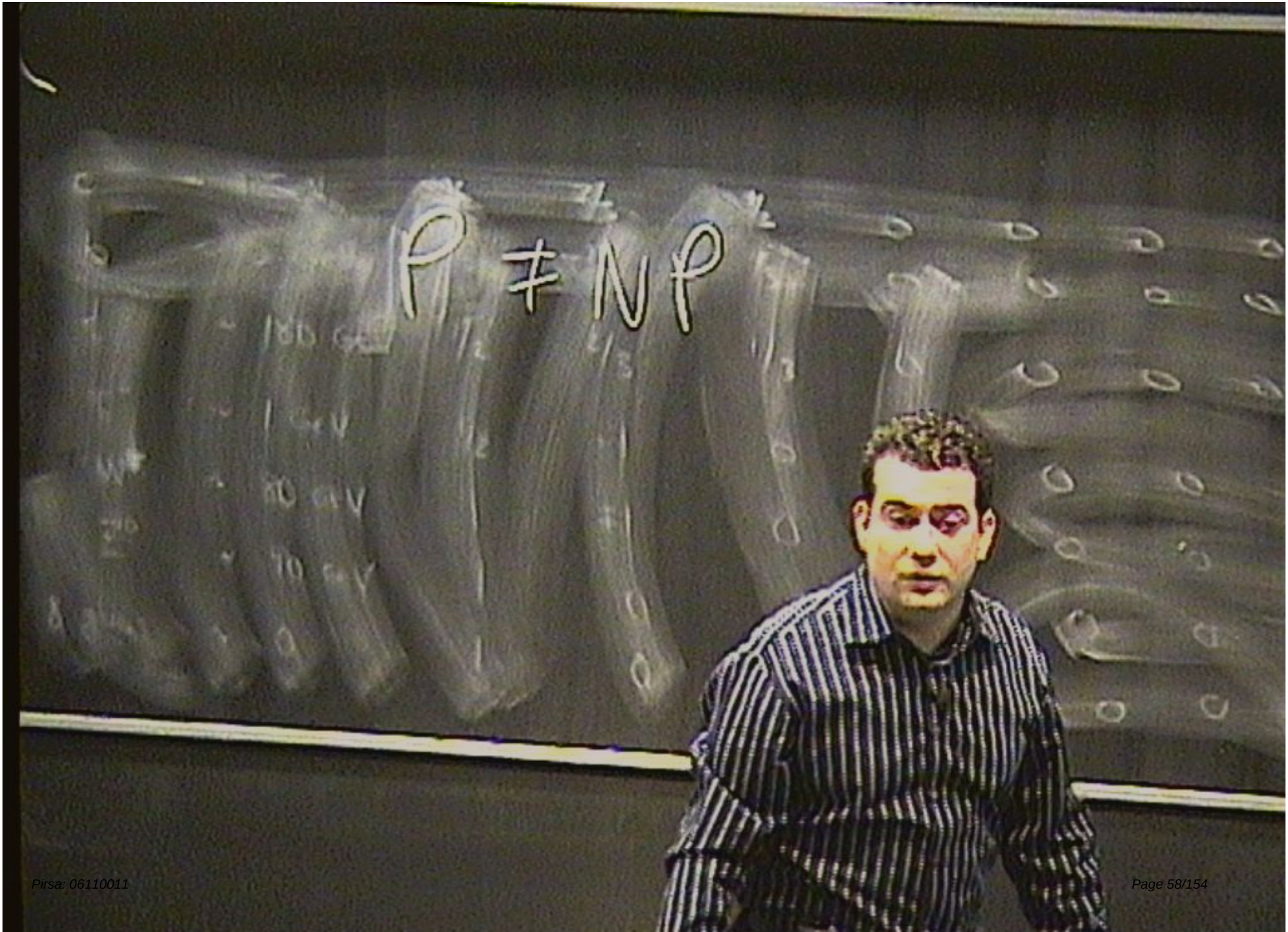
Why should you trust this result?

Why else do we want to test?

Suppose we are paying a lot of money to perform a large quantum computation, whose answer is not efficiently classically checkable.

Why should you trust this result?

Or, suppose we have proved one of the Clay Institute $1M Millennium problem by a proof that needs to be run on a quantum computer.


P ≠ NP

What else was known?

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

3) The ability to use the same gate more than once in the same experiment

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

3) The ability to use the same gate more than once in the same experiment

4) The ability to prepare and measure '0' and '1'

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

3) The ability to use the same gate more than once in the same experiment

4) The ability to prepare and measure '0' and '1'

5) The dimension of the physical systems storing the qubits was known (i.e. 2-level systems)

What else was known?

Van Dam, Magniez, M, Santha developed a series of self-tests for a universal and fault-tolerant set of quantum gates, with three additional assumptions:

3) The ability to use the same gate more than once in the same experiment

4) The ability to prepare and measure '0' and '1'

5) The dimension of the physical systems storing the qubits was known (i.e. 2-level systems)

What needs to be done?

What needs to be done?

We wish to remove assumptions 3,4 and 5.

What needs to be done?

We wish to remove assumptions 3,4 and 5.

We wish to still have a "composable" technique for self-testing a large circuit; since we want it to be efficient.

One step in that direction

What needs to be done?

We wish to remove assumptions 3,4 and 5.

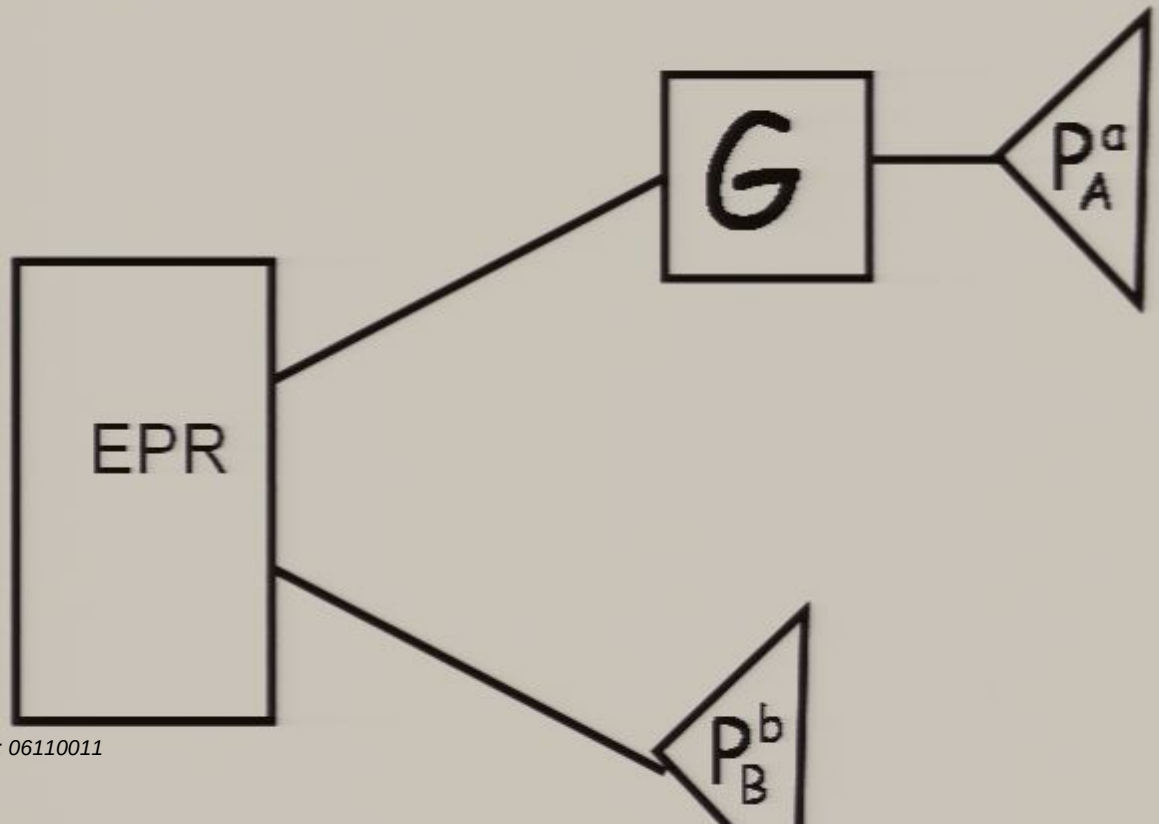
We wish to still have a "composable" technique for self-testing a large circuit; since we want it to be efficient.

One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing

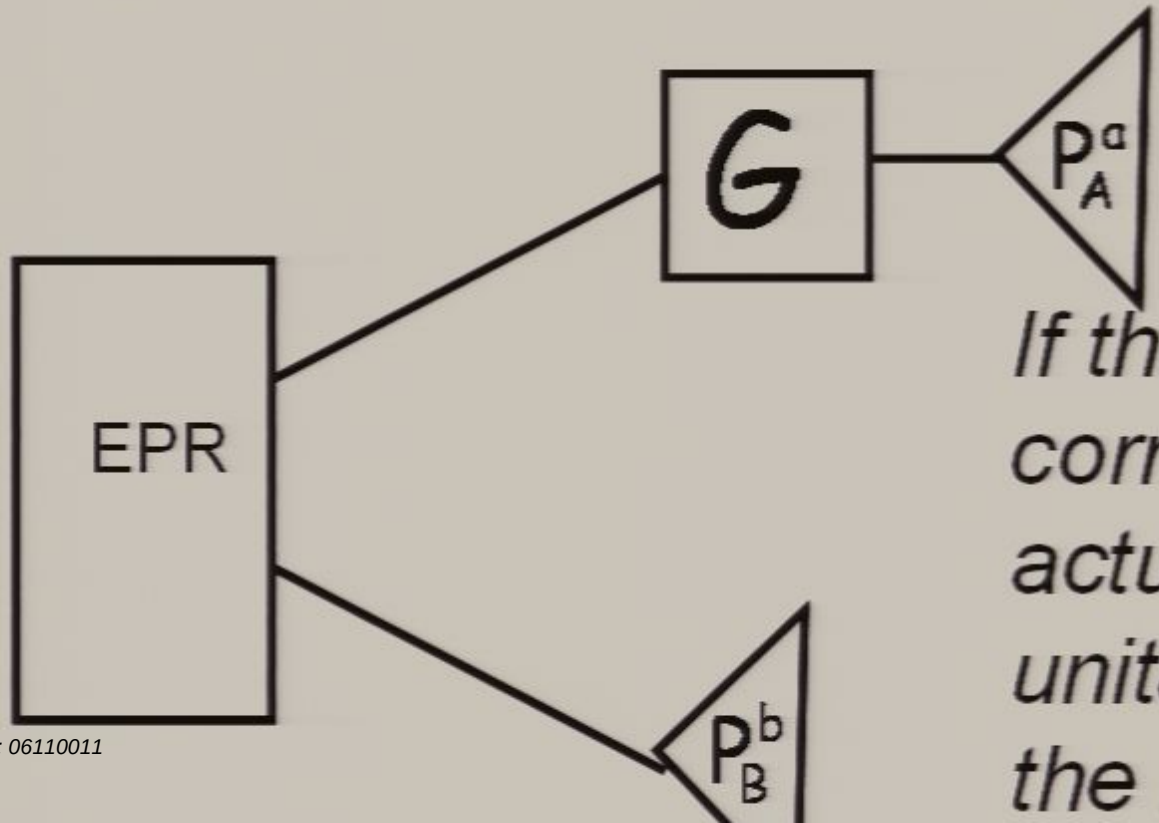
One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing



One step in that direction

We can combine the EPR self-test of Mayers-Yao with DMMS-style gate testing



If the statistics are correct, then the actual gate G is locally unitarily equivalent to the ideal gate, T.

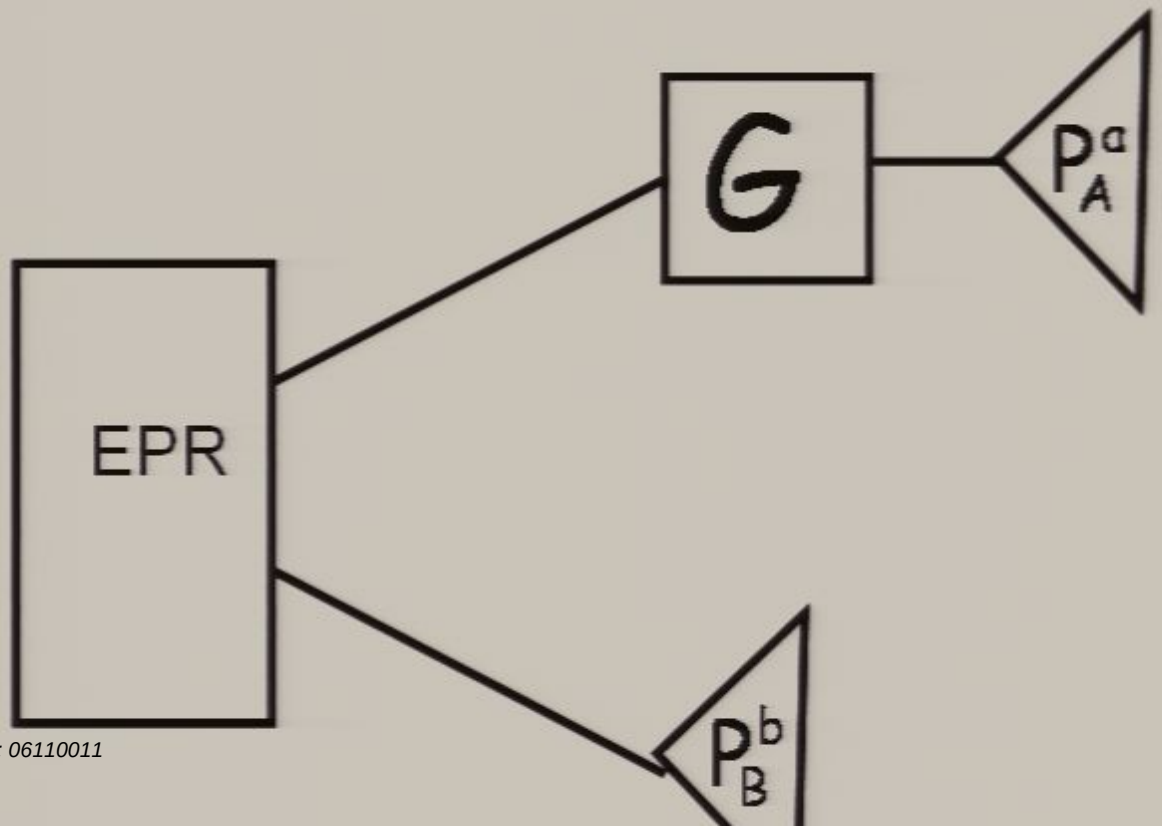
Still not composable…

Still not composable…

The following does not necessarily compose

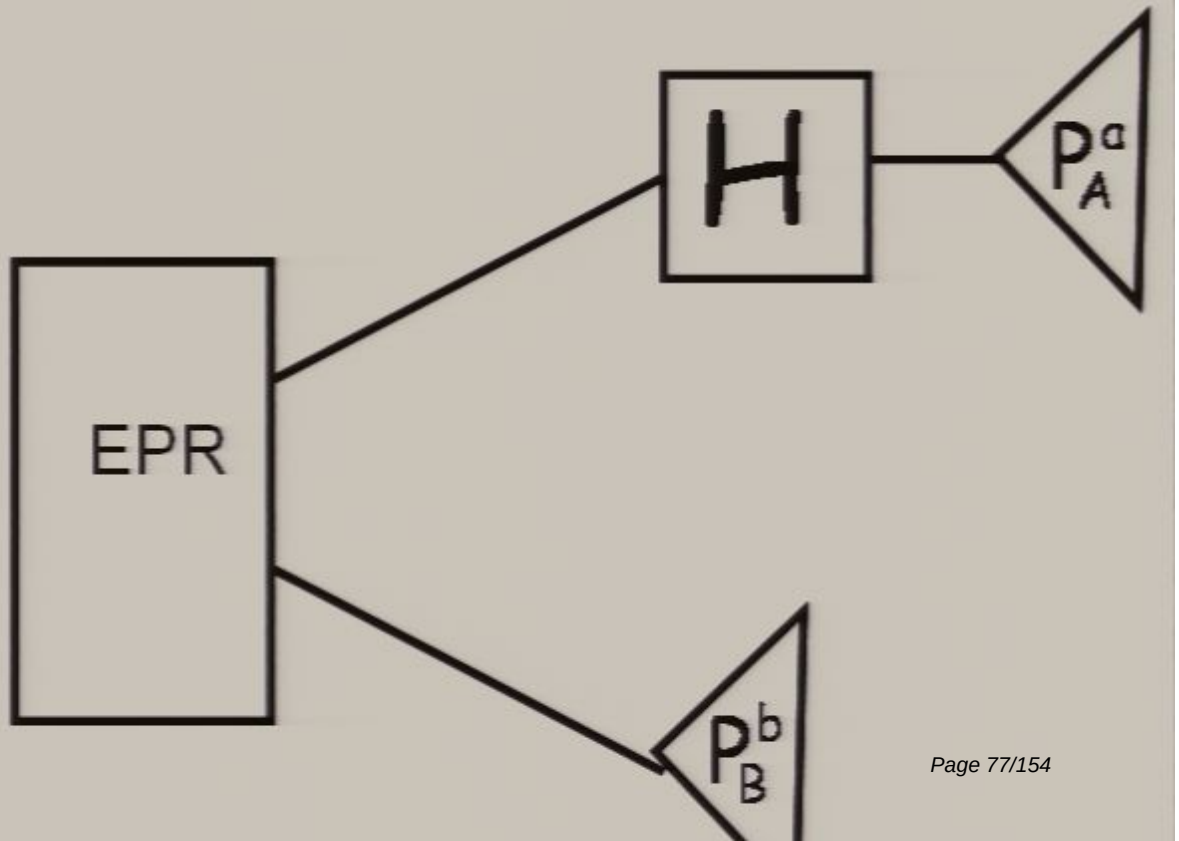
Still not composable…

The following does not necessarily compose



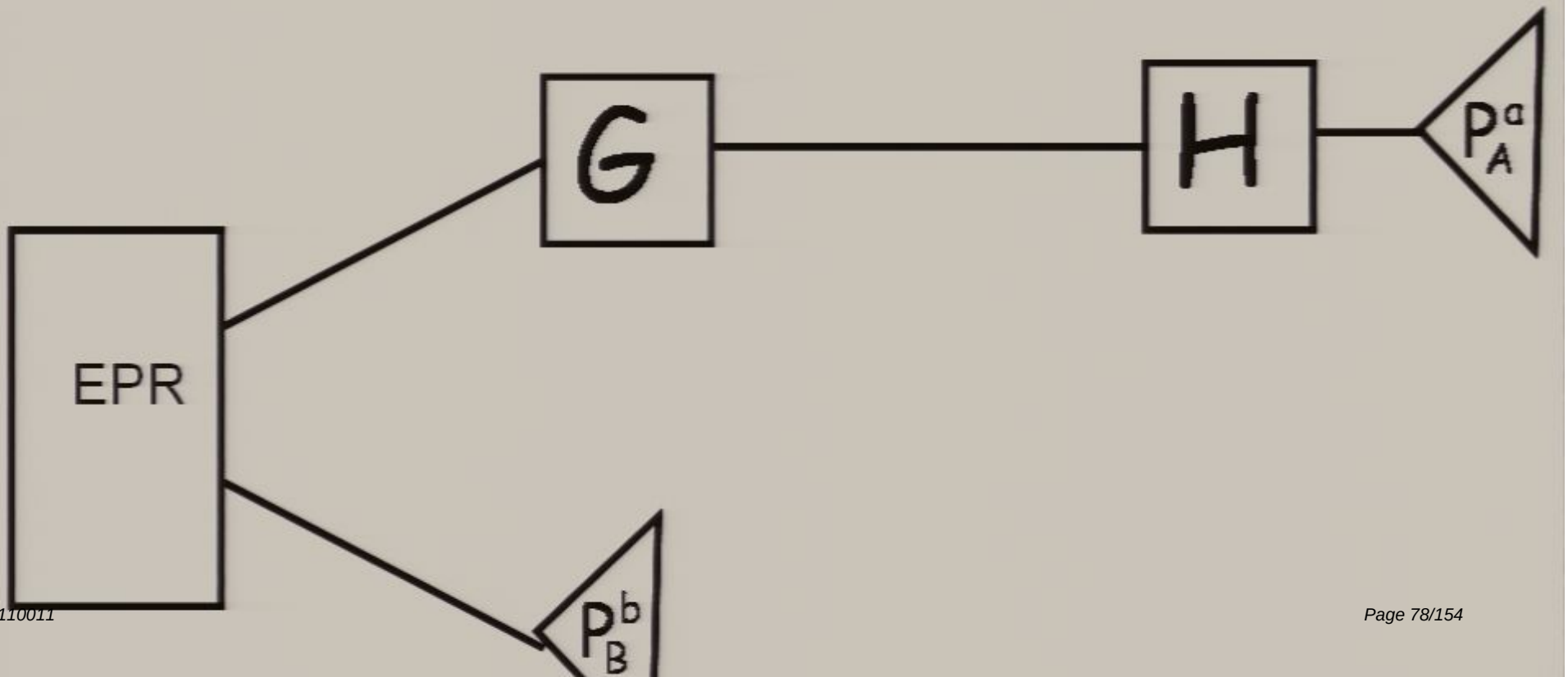
Still not composable…

The following does not necessarily compose



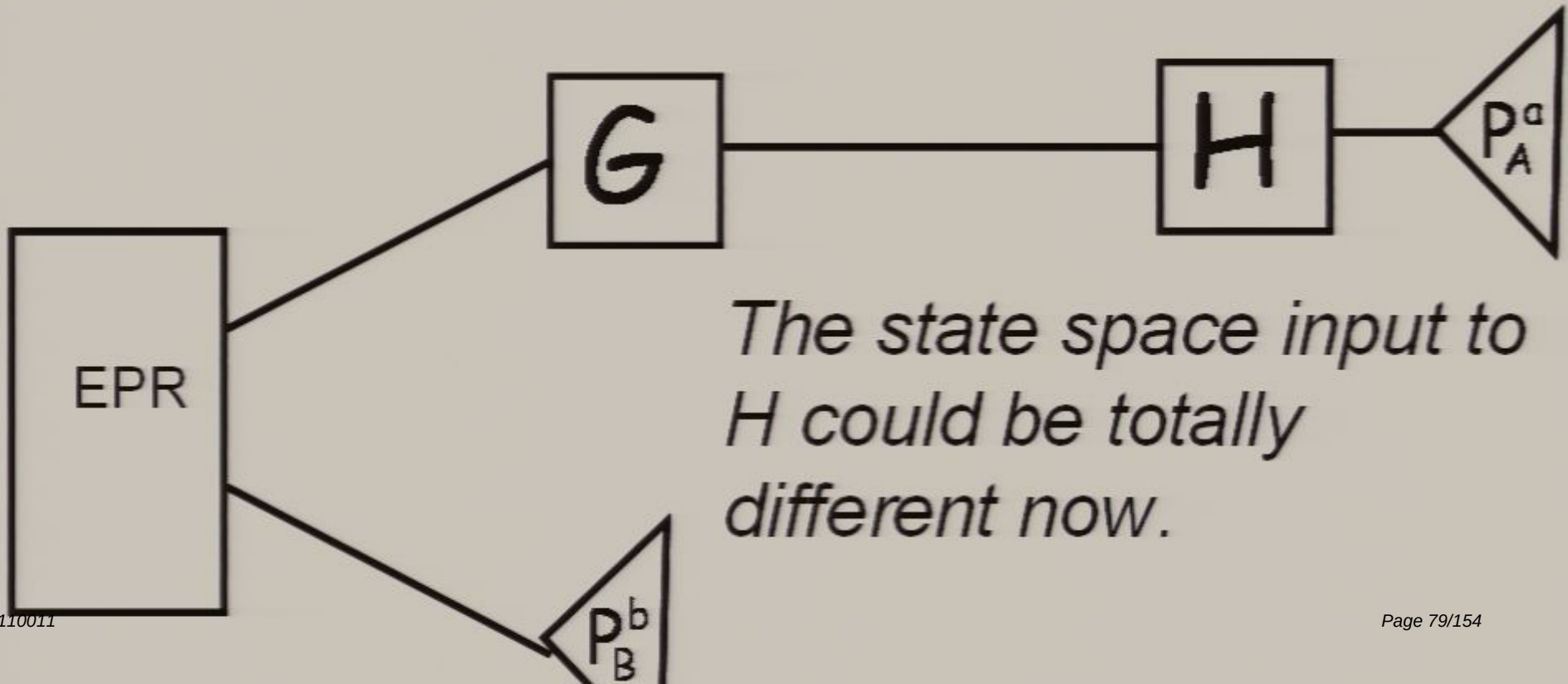
Still not composable…

The following does not necessarily compose



Still not composable…

The following does not necessarily compose



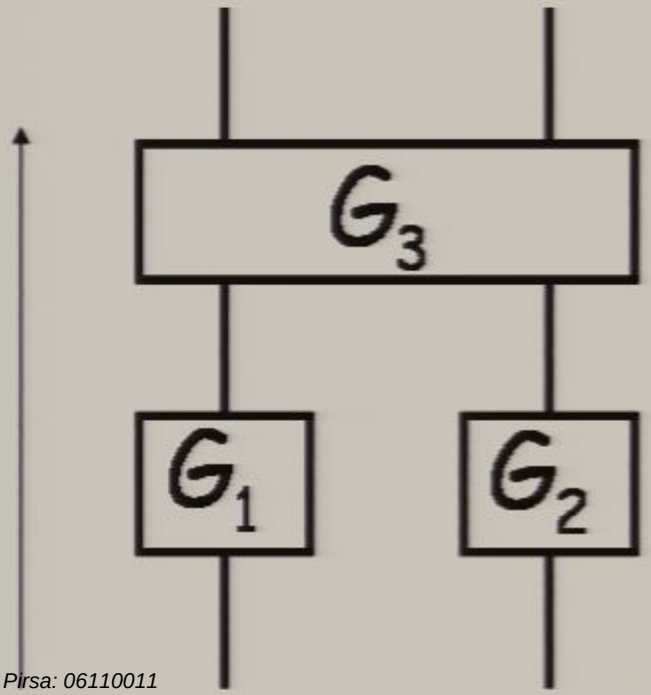
The state space input to H could be totally different now.

Goal

We ultimately wish to test the performance of an entire circuit *(note that the circuits now flow up)*

Goal

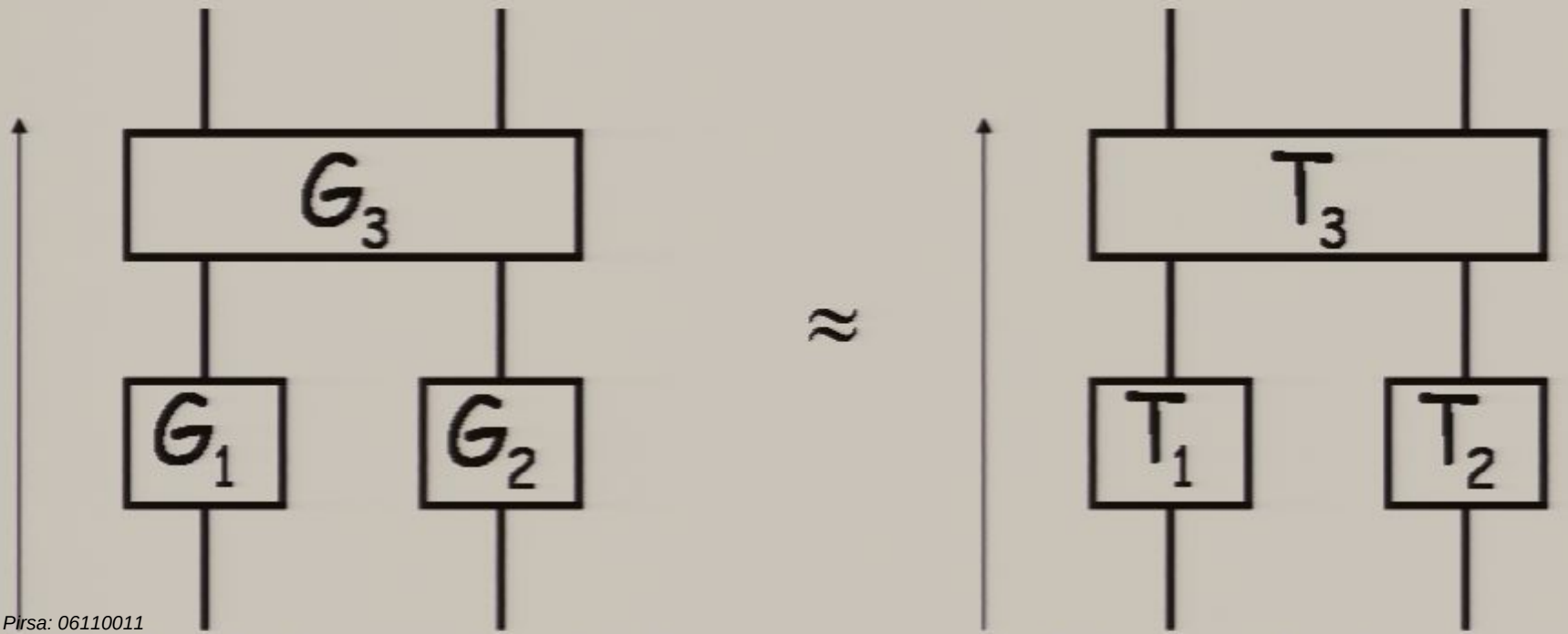
We ultimately wish to test the performance of an entire circuit *(note that the circuits now flow up)*



"actual physical gates"

Goal

We ultimately wish to test the performance of an entire circuit *(note that the circuits now flow up)*



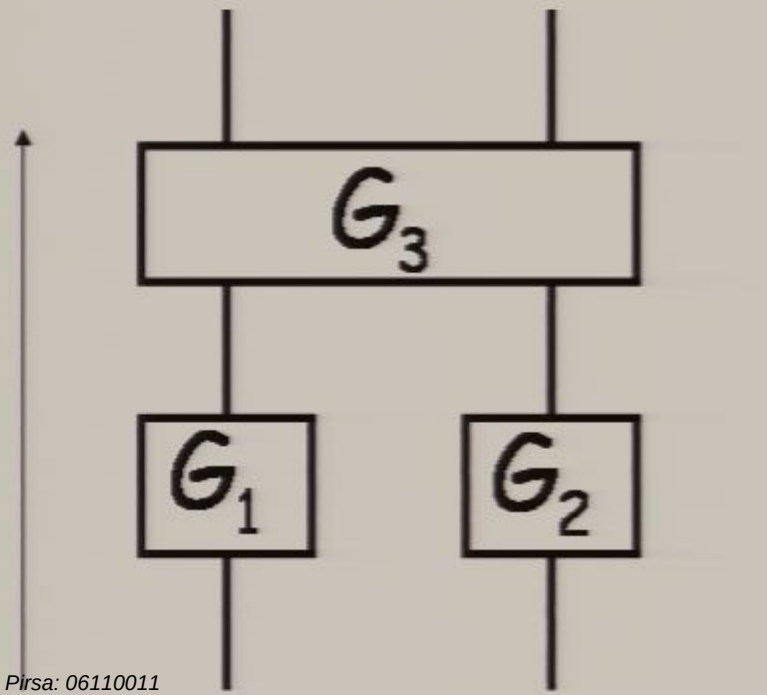
"actual physical gates" *"ideal gates"*

example

Suppose we wish to run the following circuit

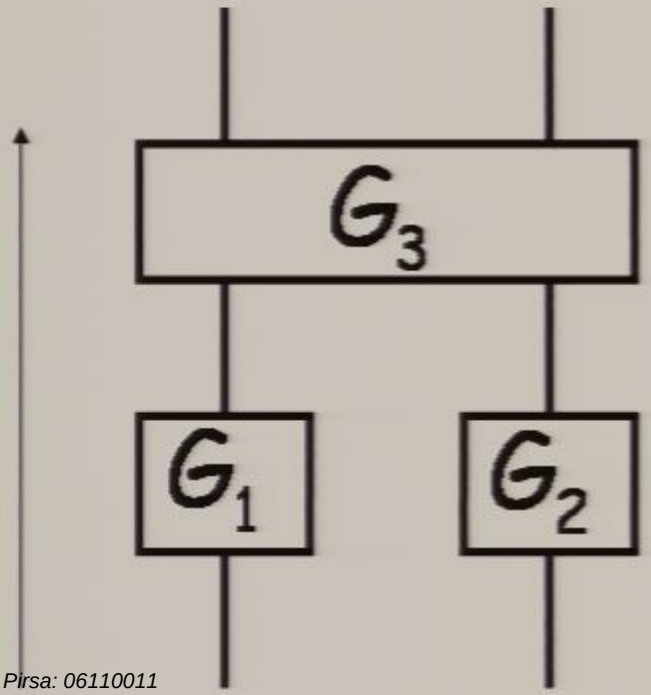
example

Suppose we wish to run the following circuit



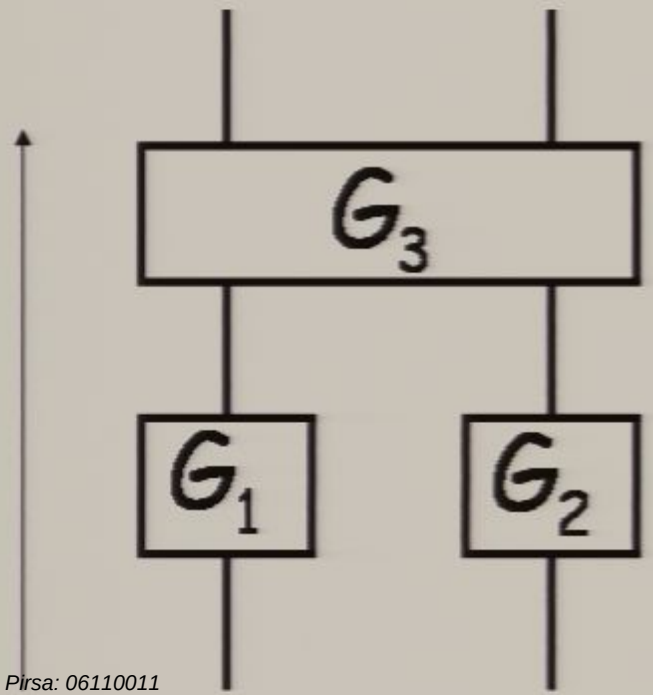
example

Suppose we wish to run the following circuit



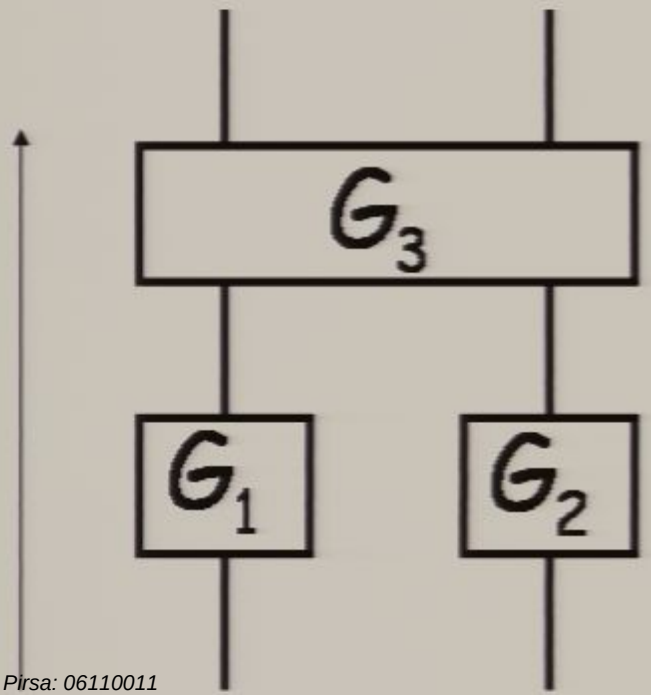
example

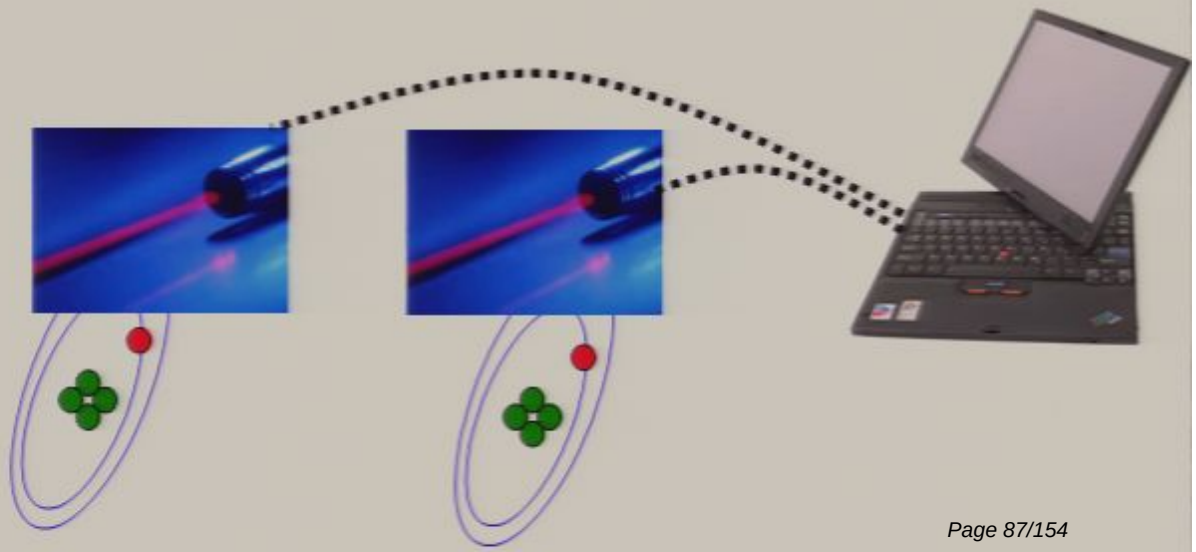
Suppose we wish to run the following circuit



example

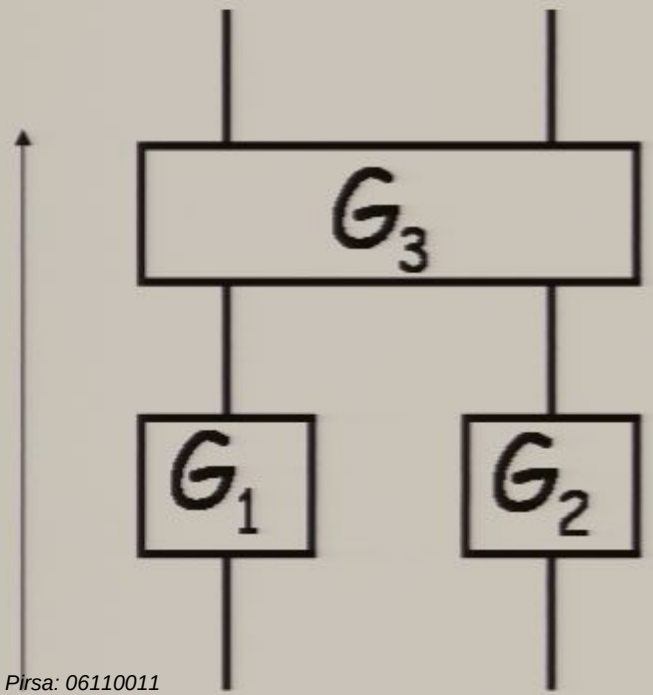
Suppose we wish to run the following circuit





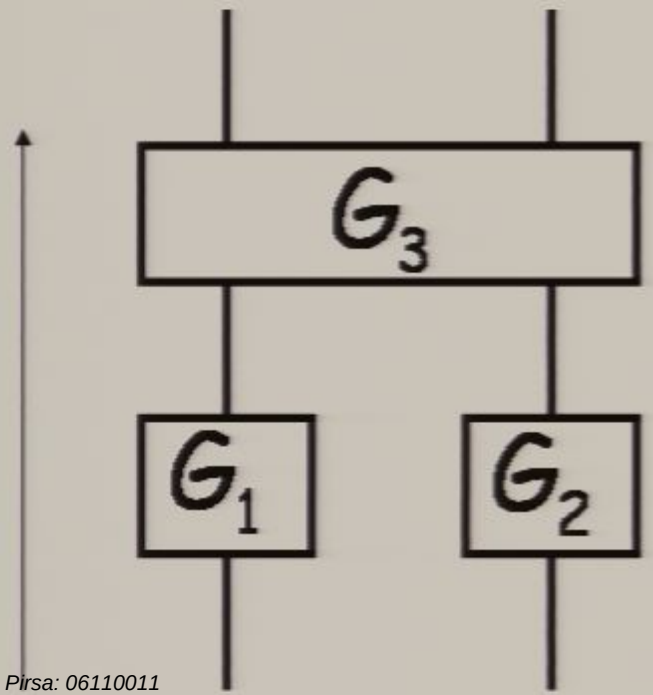
example

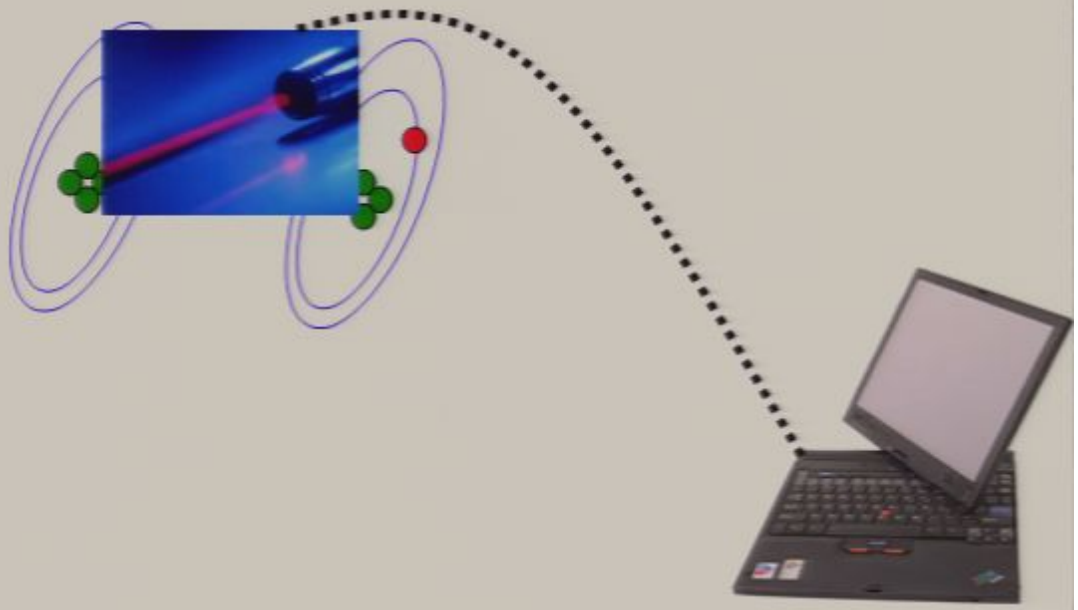
Suppose we wish to run the following circuit



example

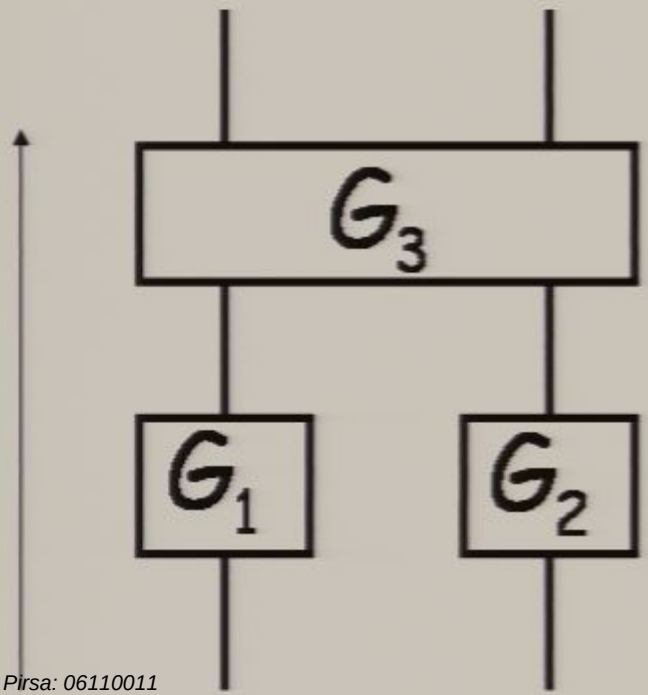
Suppose we wish to run the following circuit

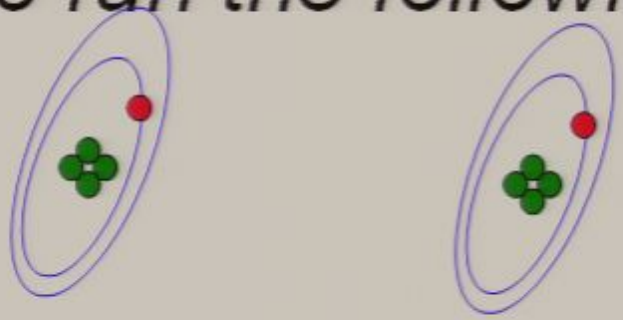




example

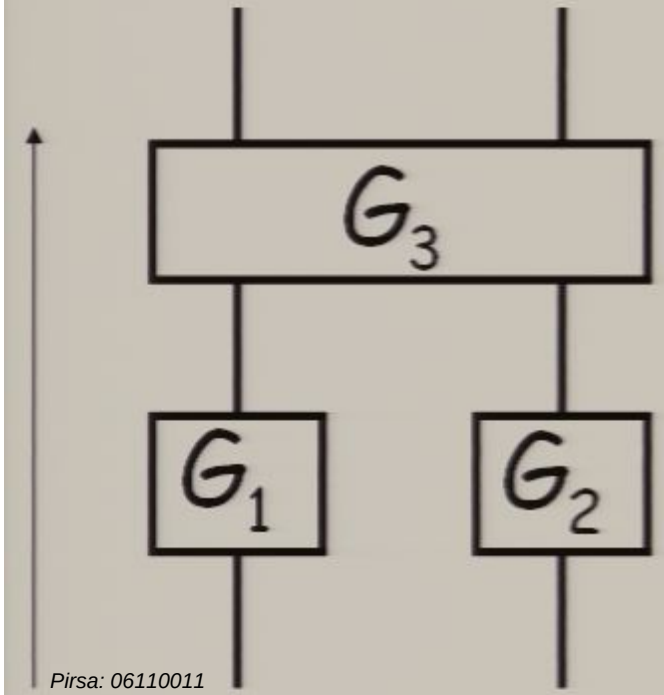
Suppose we wish to run the following circuit

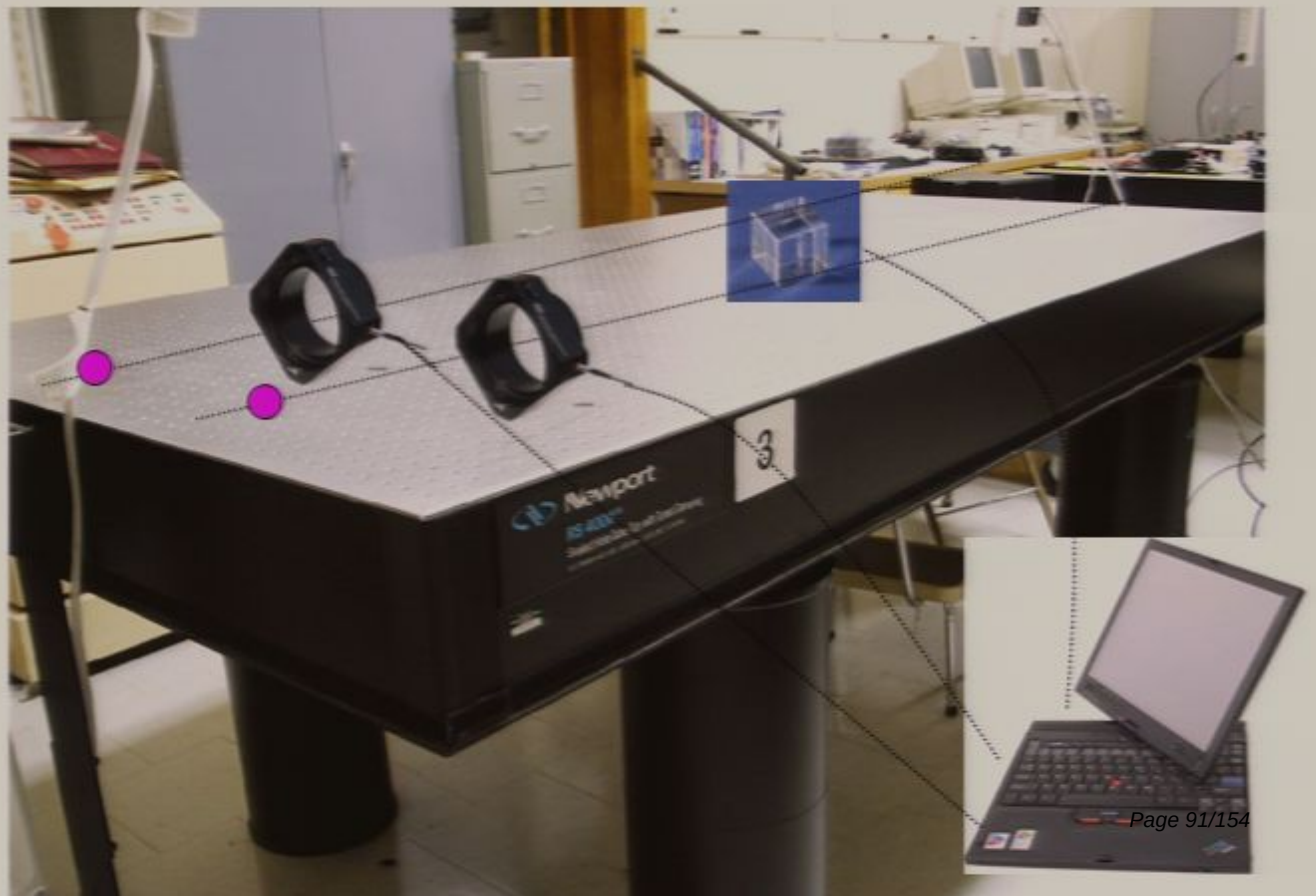




Example 2

Suppose we wish to run the following circuit





Another major challenge

Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

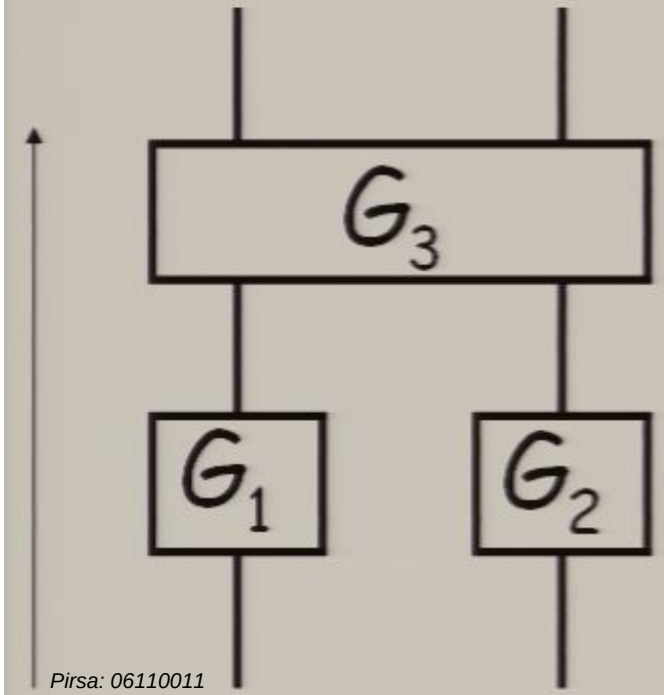
Another major challenge

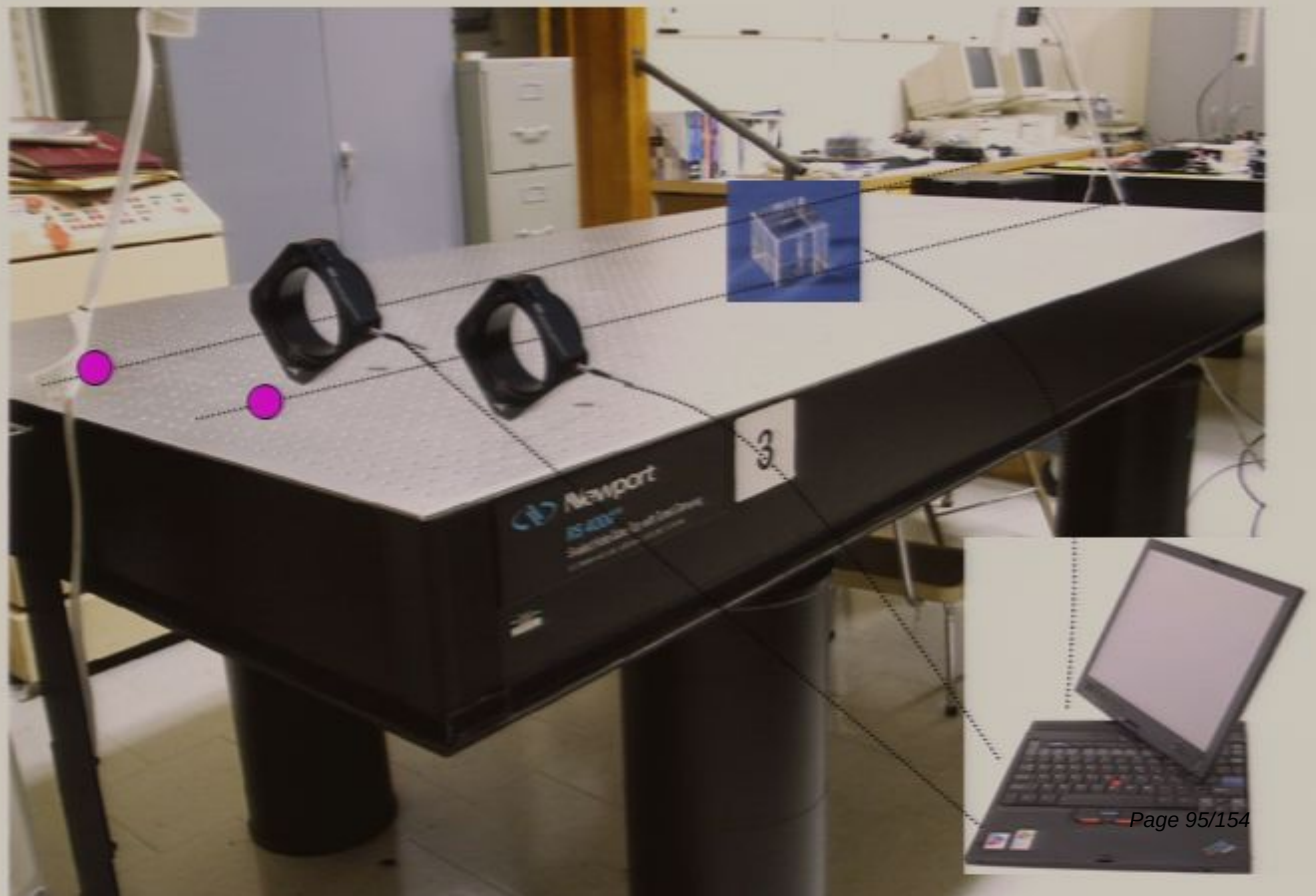
No finite set of tests will lead to a foolproof test. Why not?

The gates can pass on the full (classical) history of their past to future gates in hidden degrees of freedom. Thus each gate knows the history of its input qubit(s), and can recognize when its history is no longer part of a test.

Example 2

Suppose we wish to run the following circuit





Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

The gates can pass on the full (classical) history of their past to future gates in hidden degrees of freedom. Thus each gate knows the history of its input qubit(s), and can recognize when its history is no longer part of a test.

Hint: Every circuit we would wish to run needs to also be part of a test.

Another major challenge

No finite set of tests will lead to a foolproof test. Why not?

The gates can pass on the full (classical) history of their past to future gates in hidden degrees of freedom. Thus each gate knows the history of its input qubit(s), and can recognize when its history is no longer part of a test.

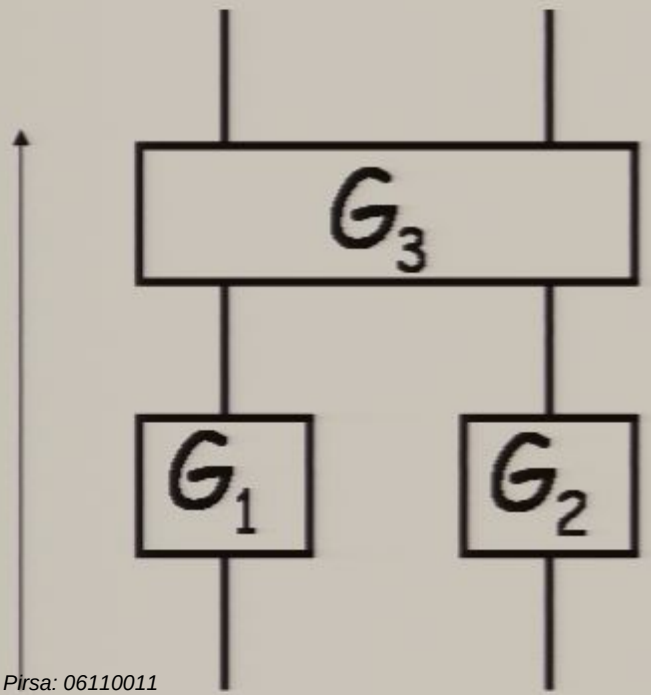
Hint: Every circuit we would wish to run needs to also be part of a test.

example

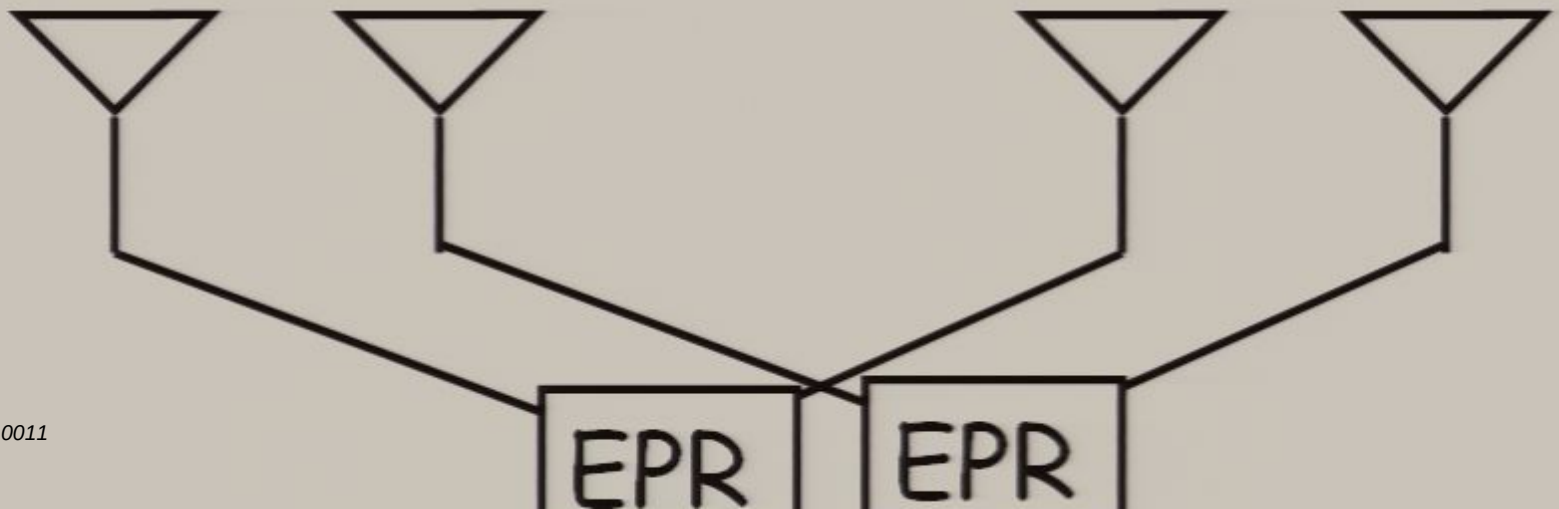
Suppose we wish to run the following circuit

example

Suppose we wish to run the following circuit

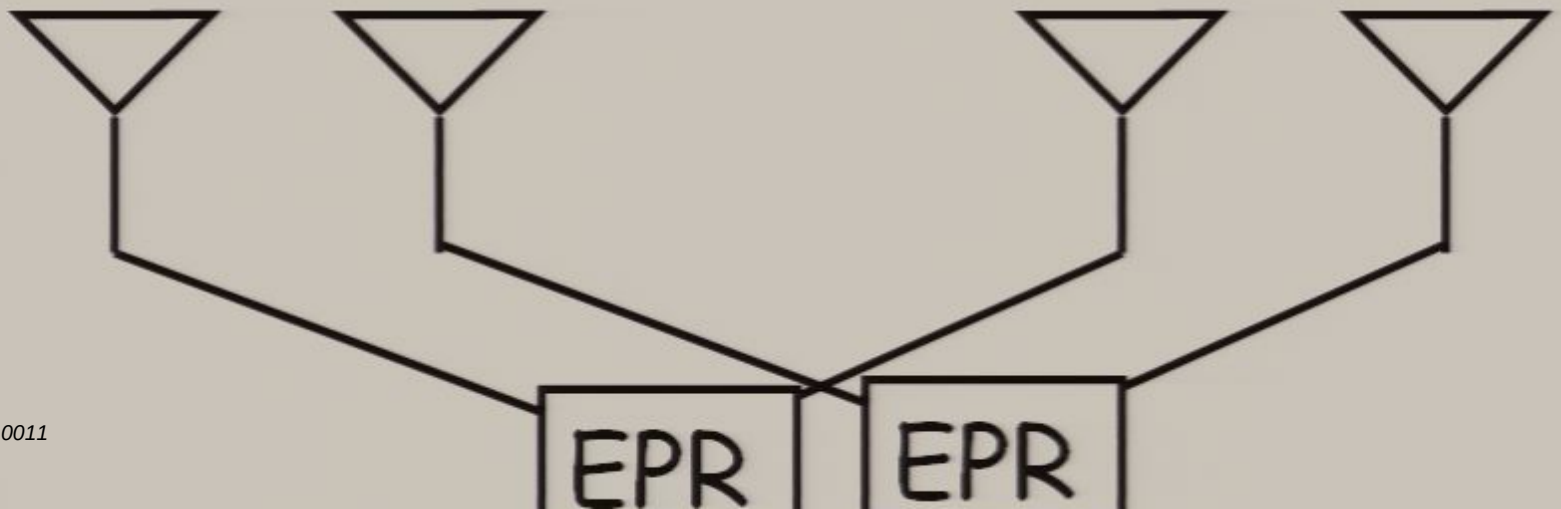


example

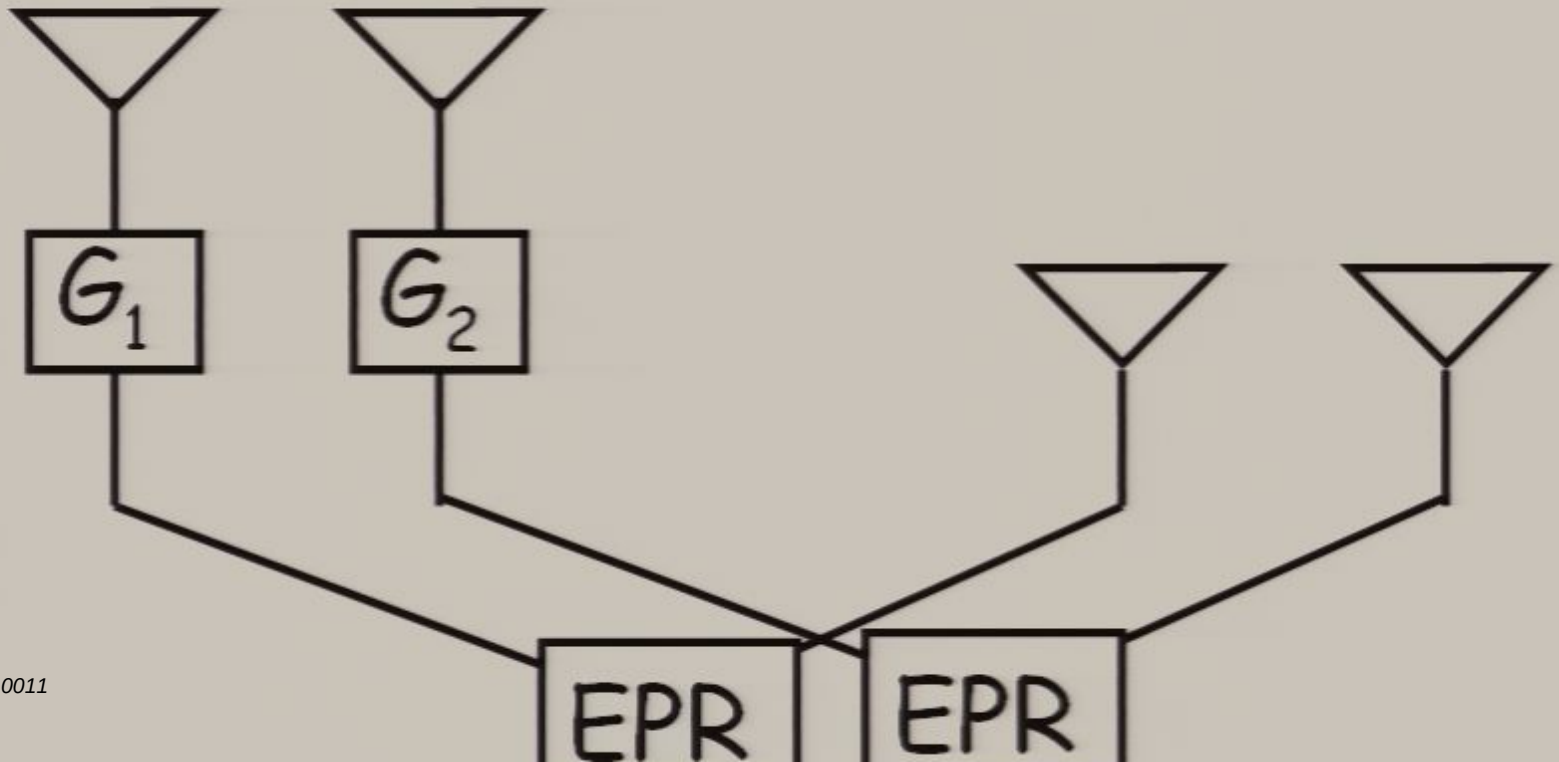


example

Verify the initial qubit sources.

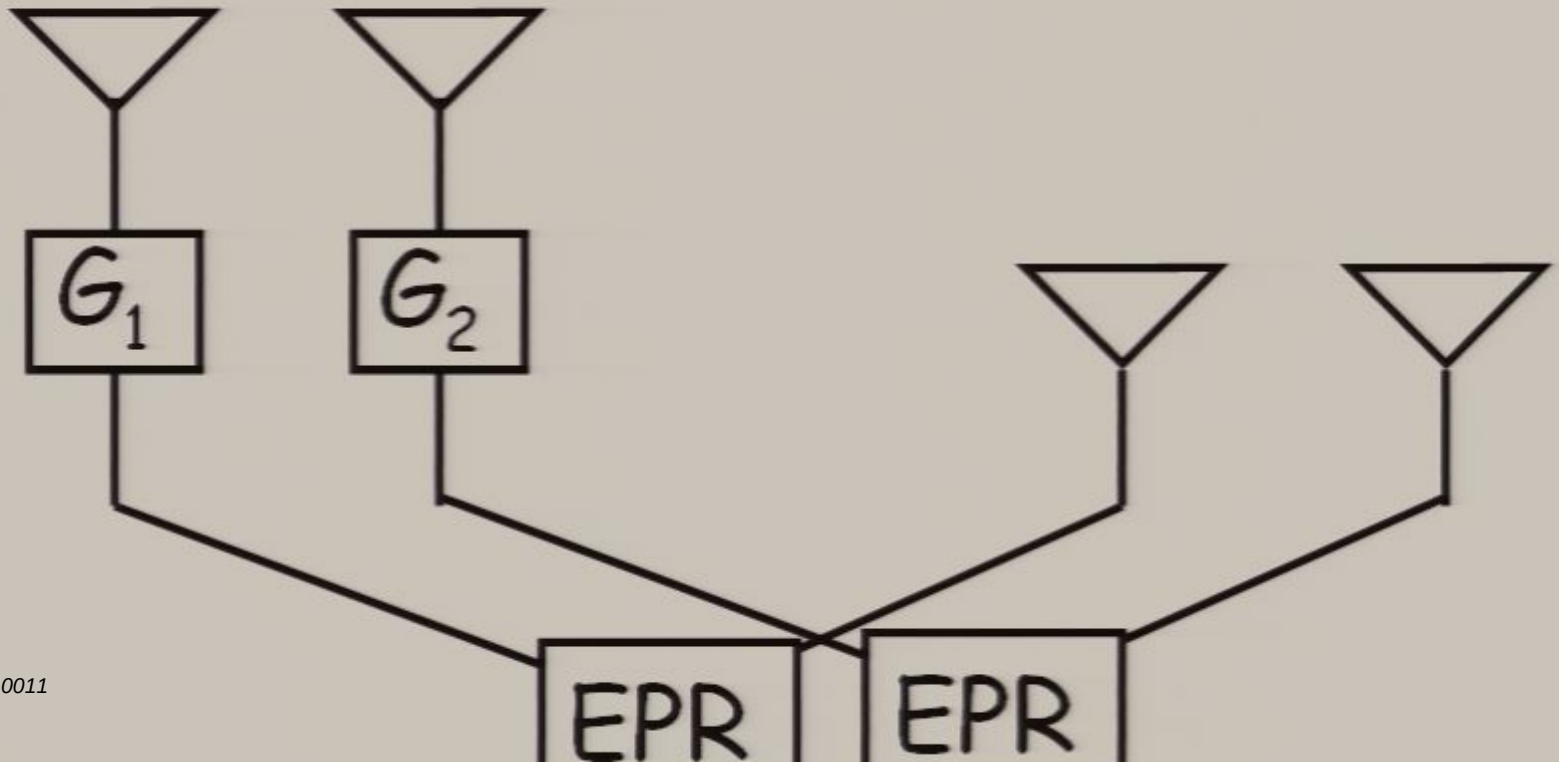


“tomography test”

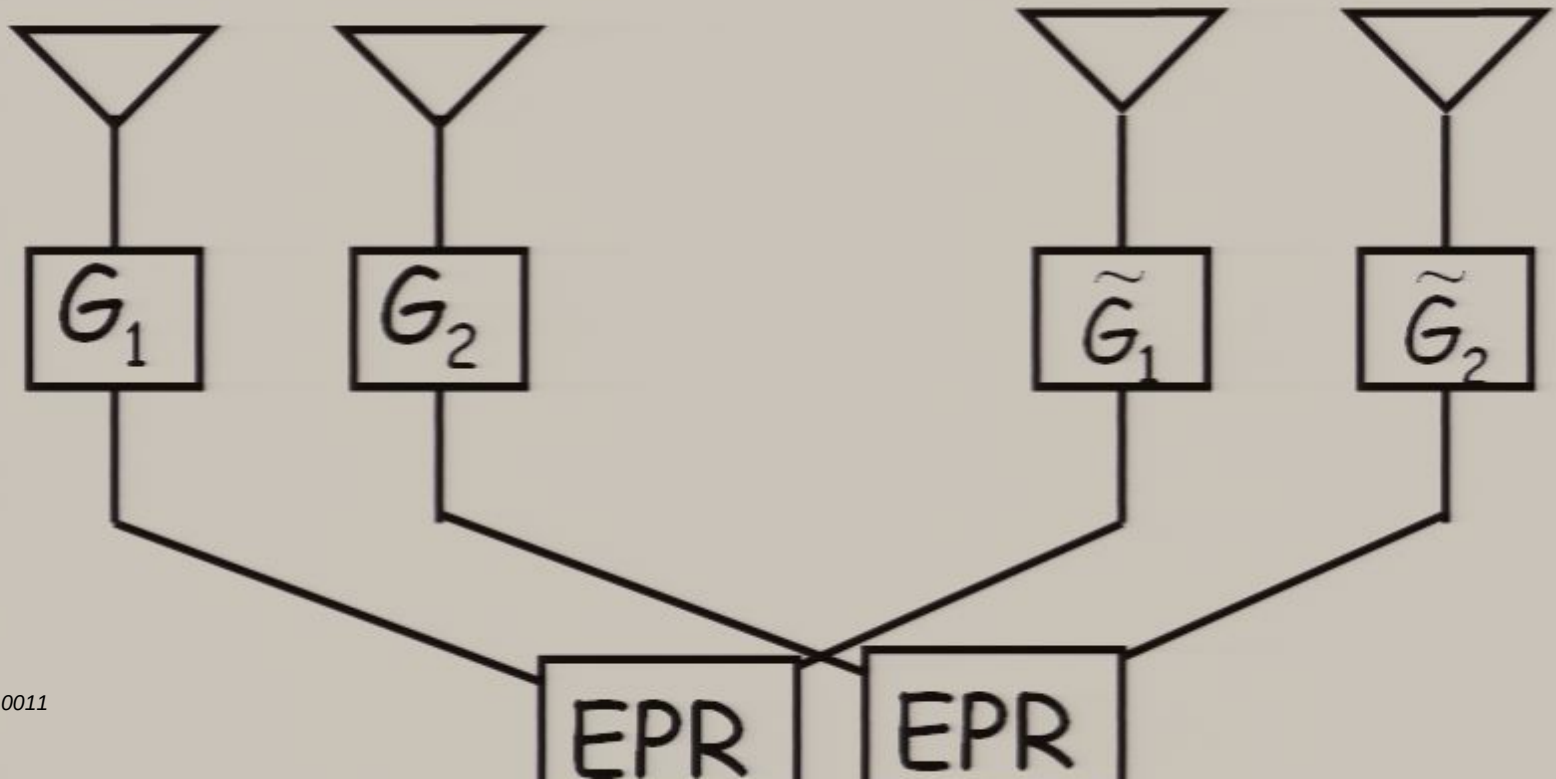


“tomography test”

We verify the behaviour of the gates G_1 and G_2

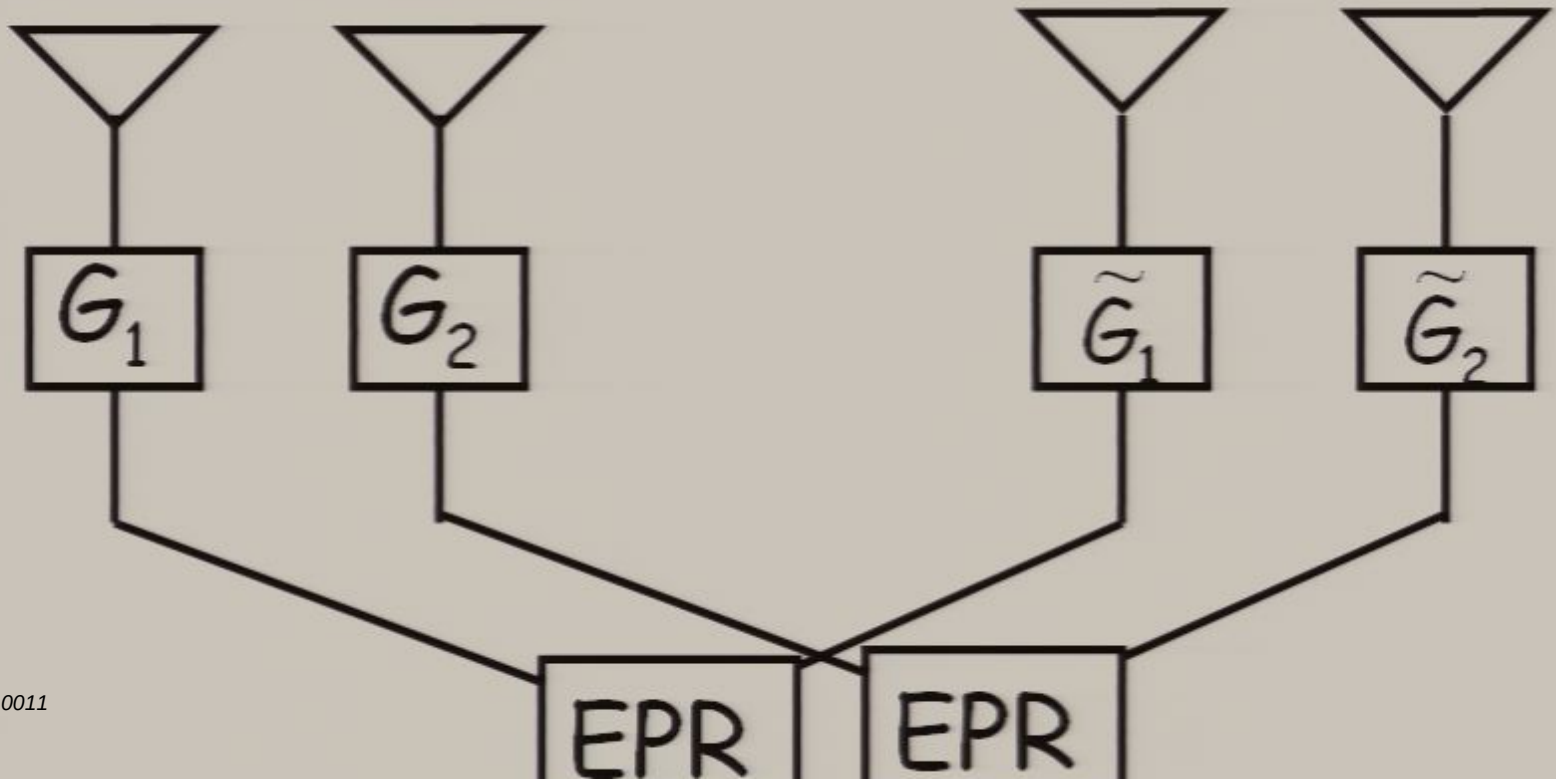


“conspiracy test”

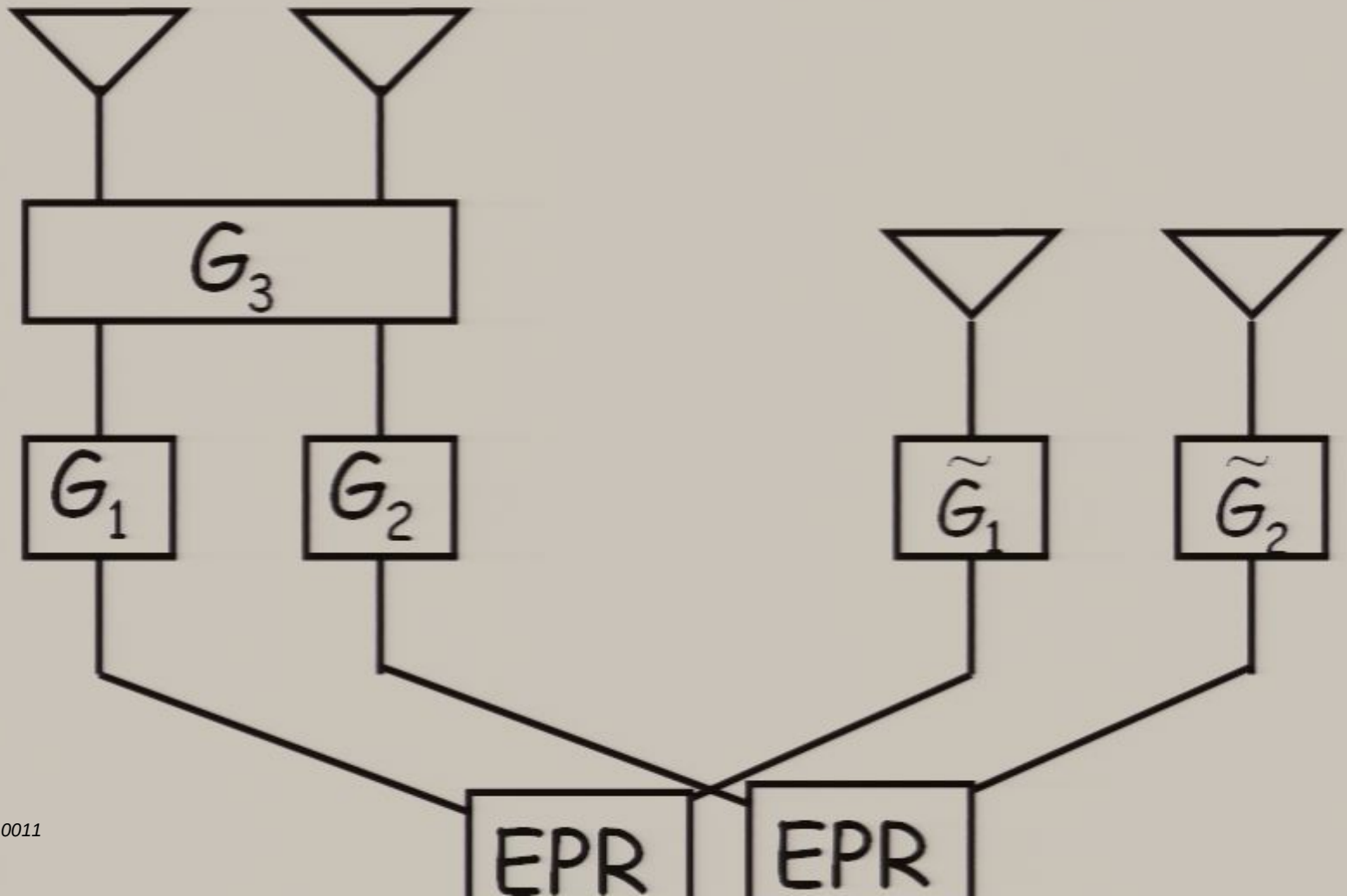


"conspiracy test"

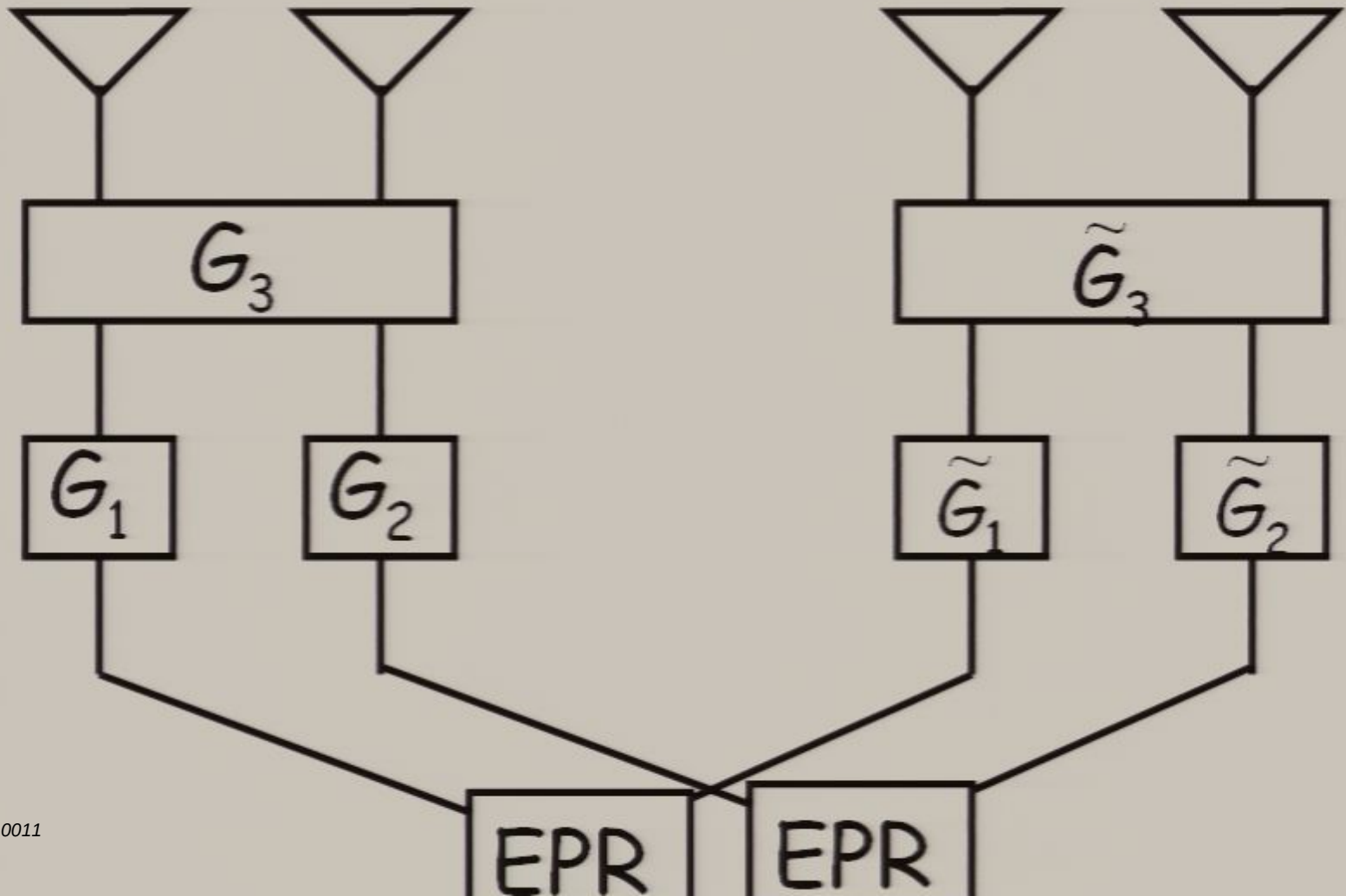
If $\tilde{G}_1 = G_1^{\dagger}$, *then this should recreate two EPR pairs.*



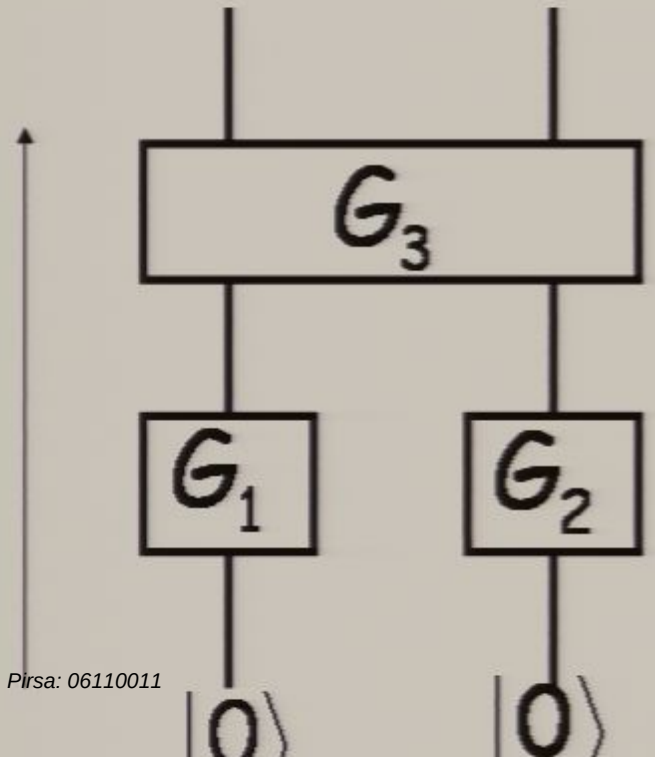
Tomography test



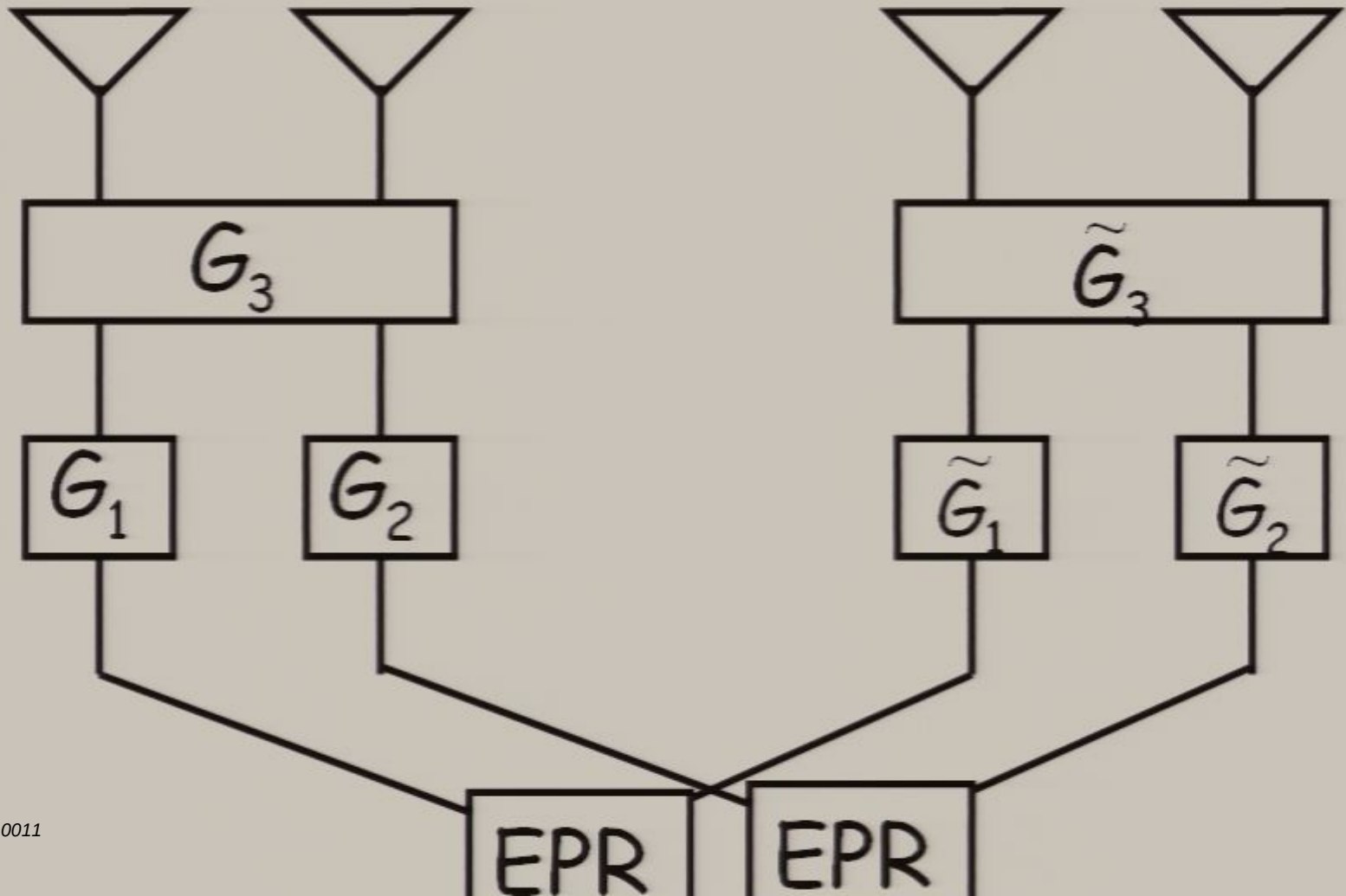
Conspiracy test



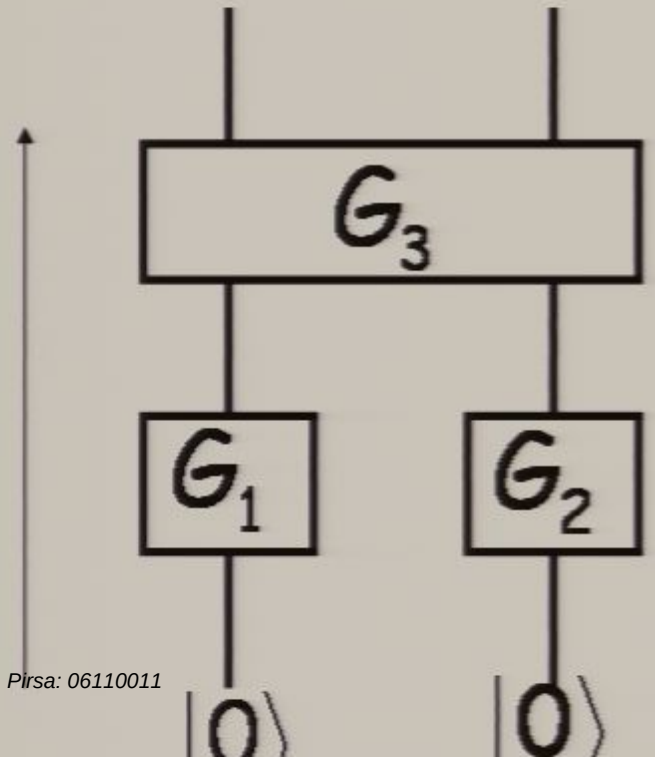
One last technical glitch



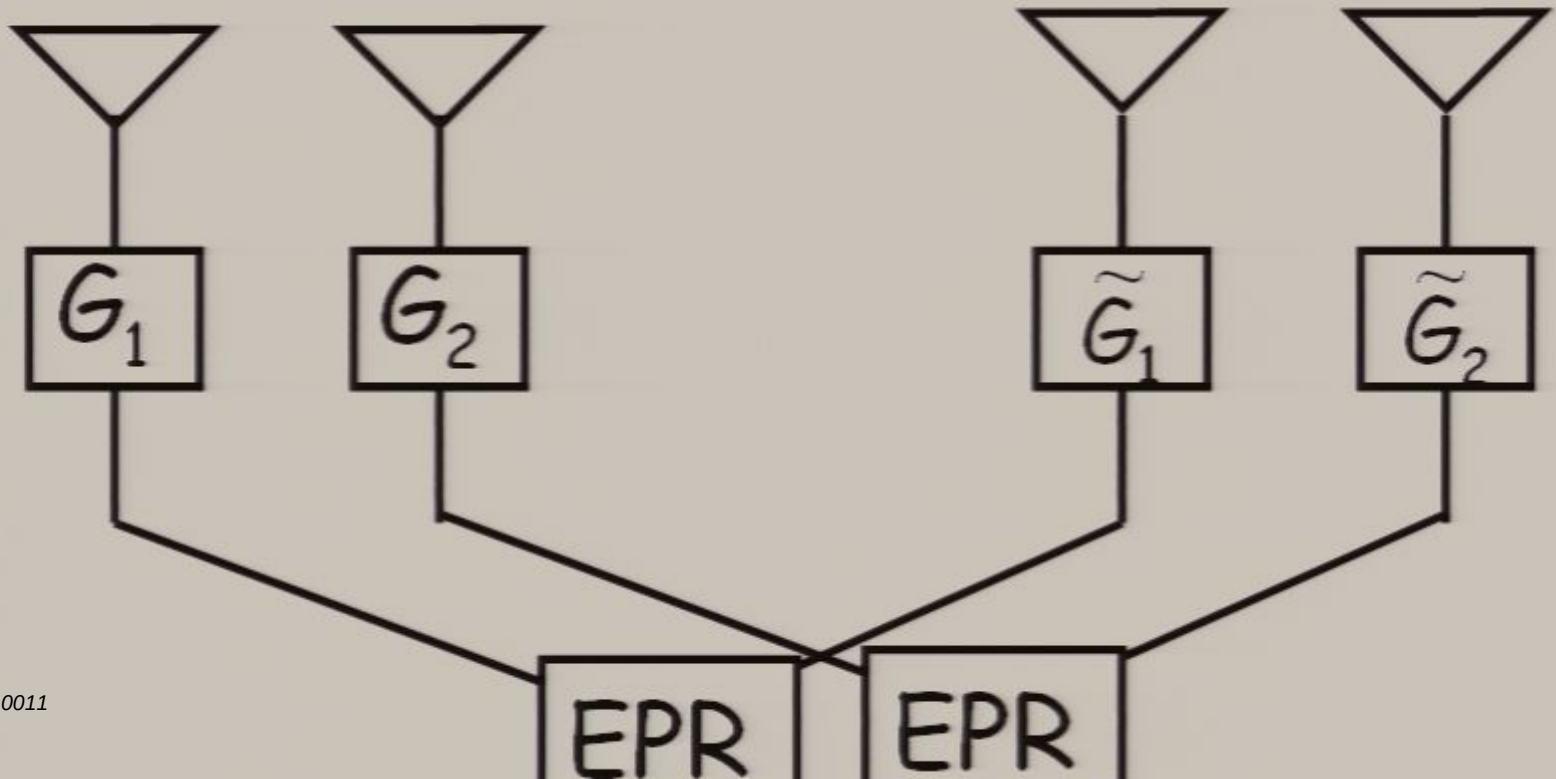
Conspiracy test



One last technical glitch

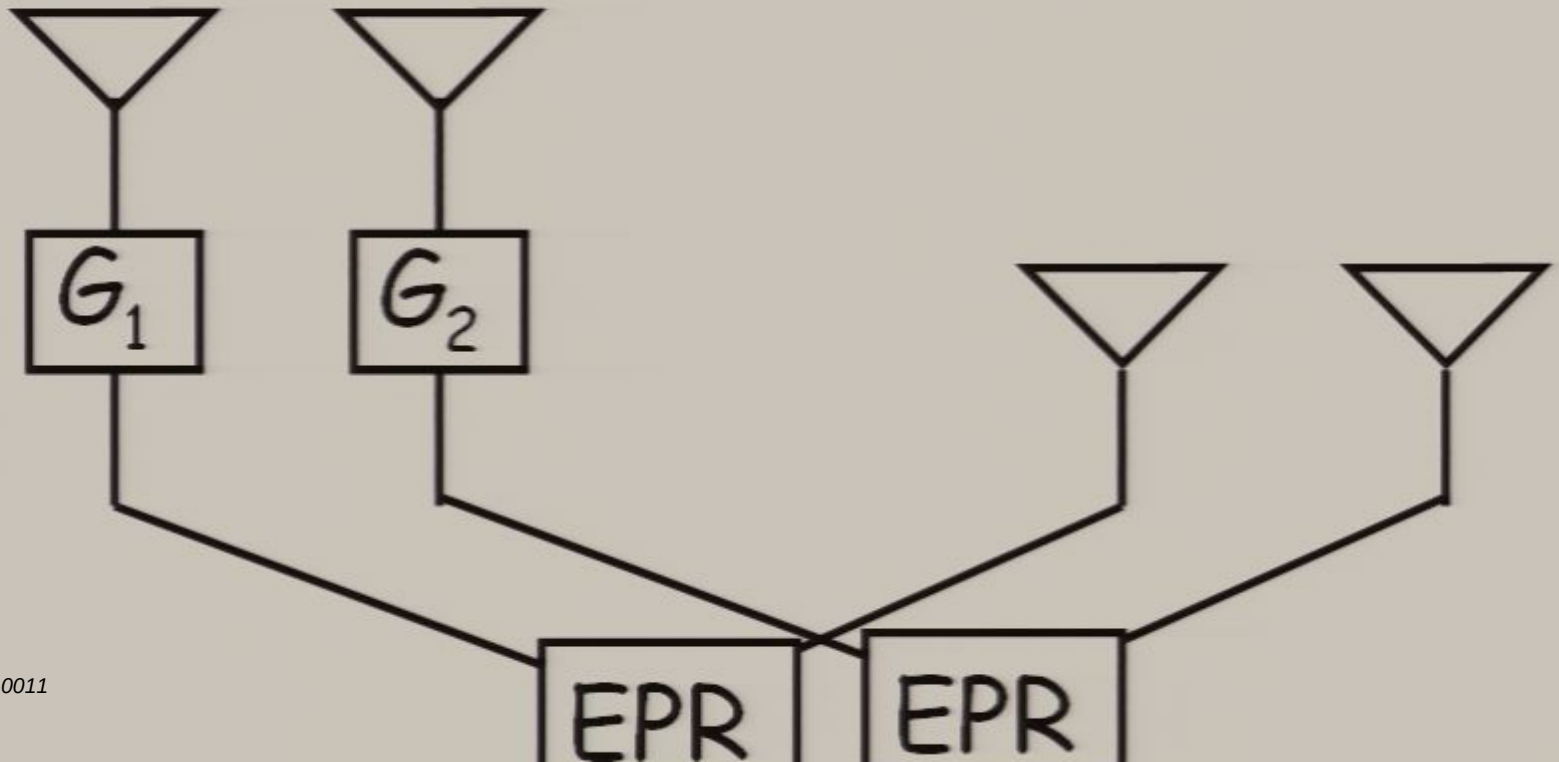


“conspiracy test”

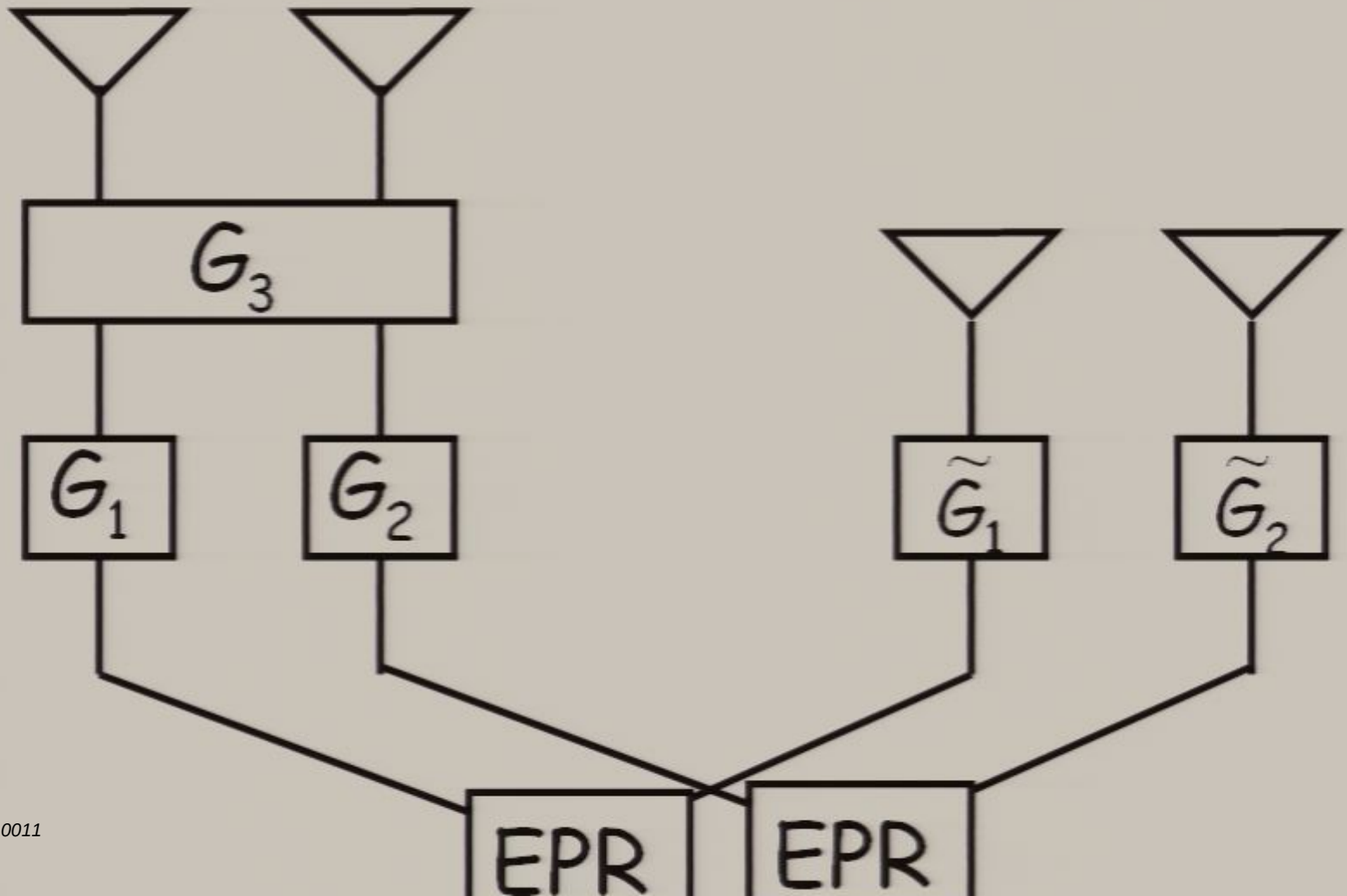


“tomography test”

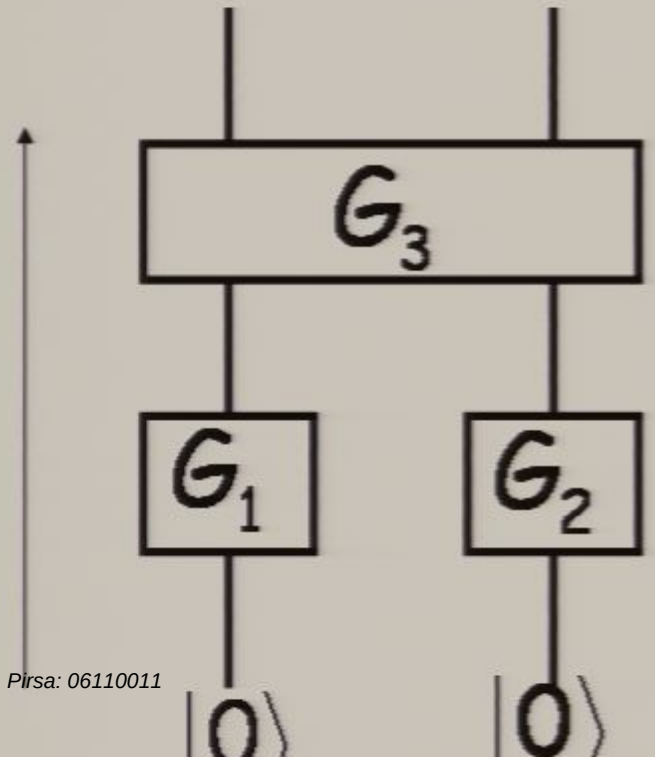
We verify the behaviour of the gates G_1 and G_2



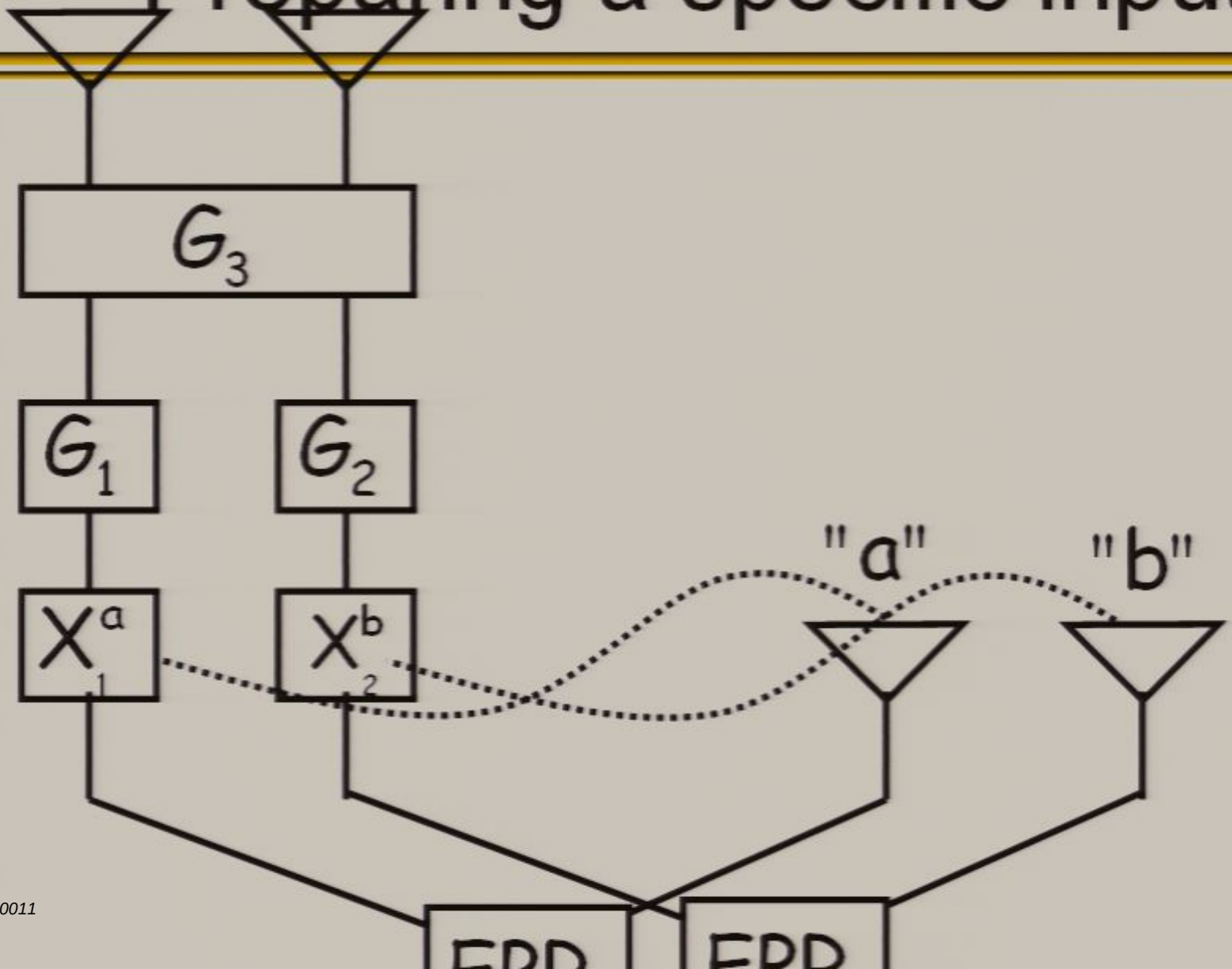
Tomography test



One last technical glitch

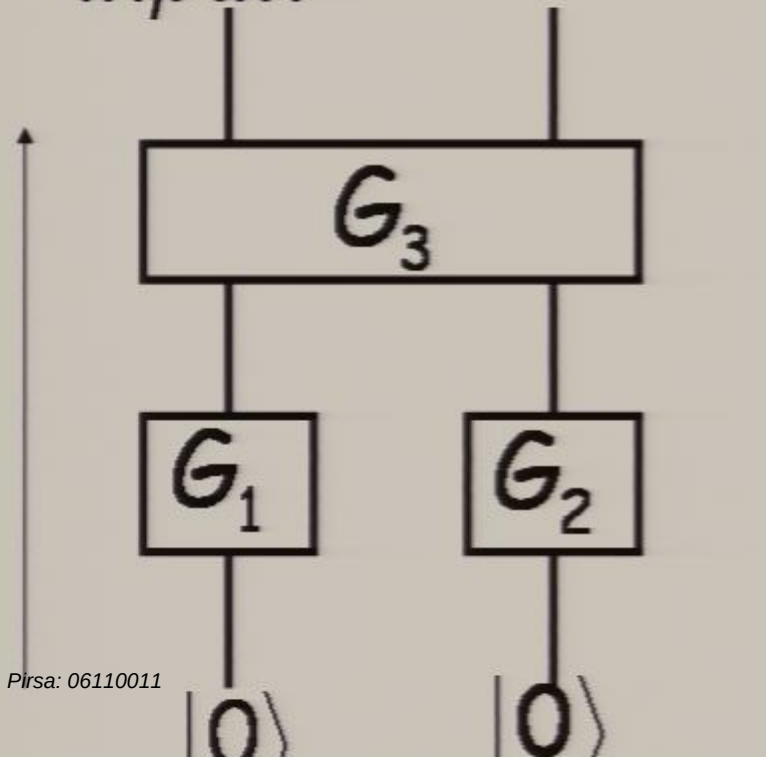


Preparing a specific input



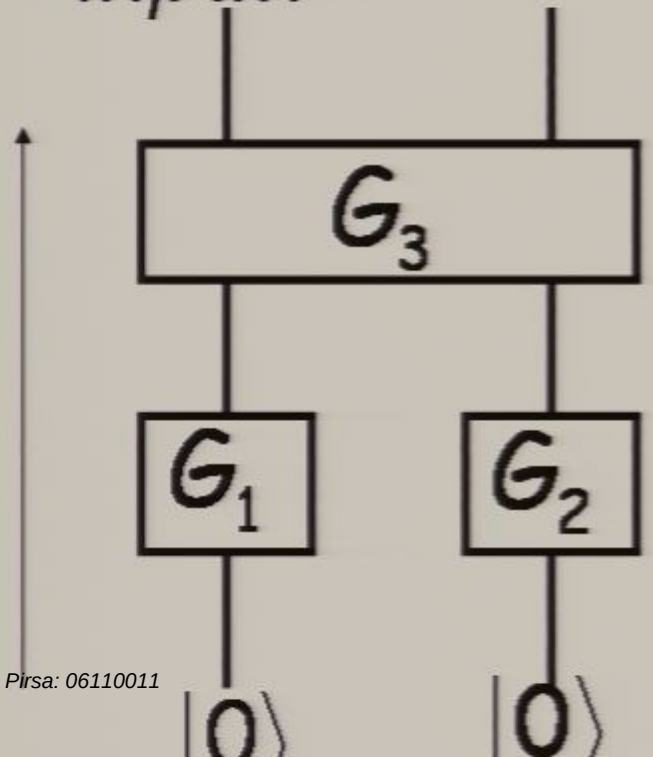
One last technical glitch

This procedure verifies the behaviour of the circuit, but how do we run it on a specific input?

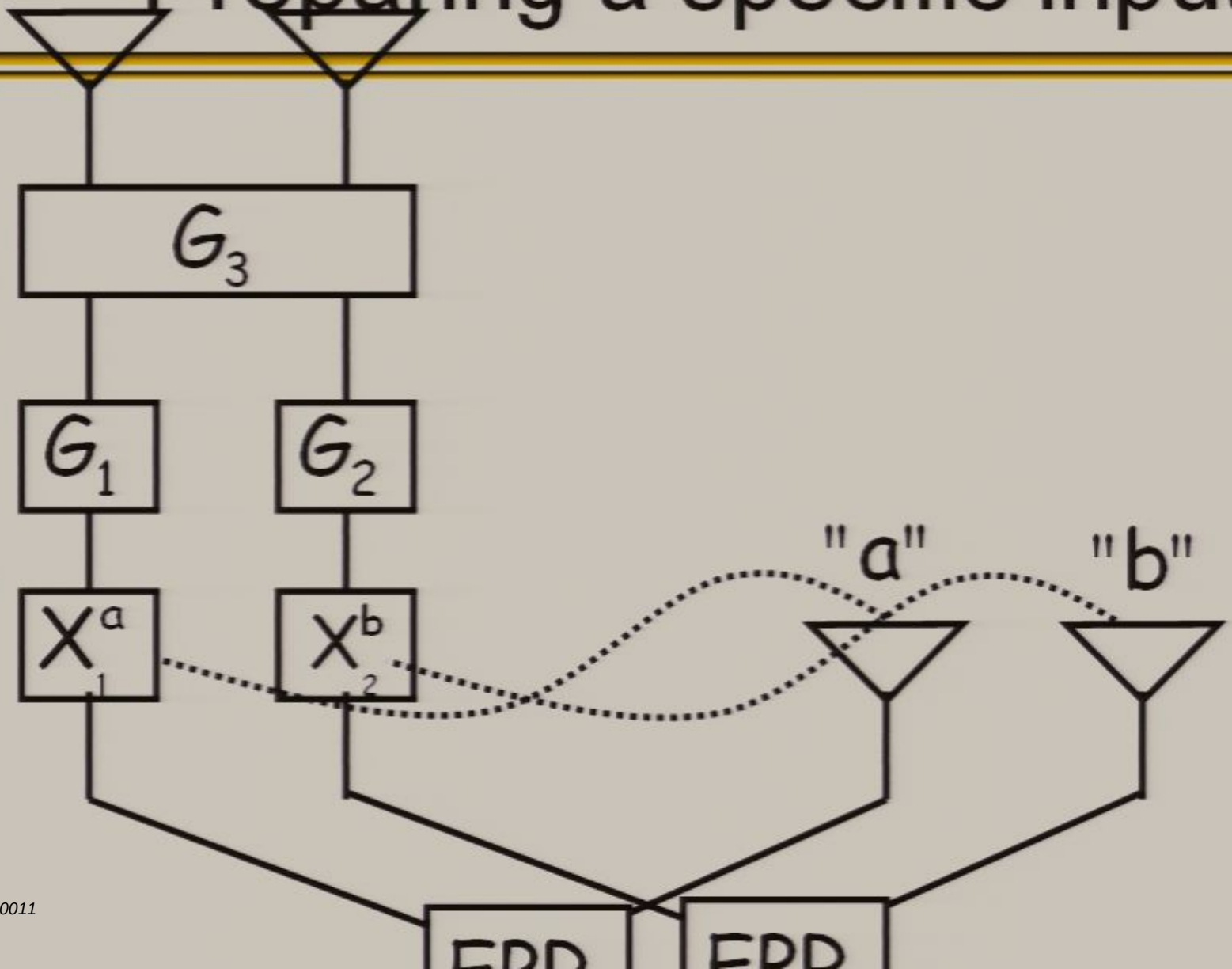


One last technical glitch

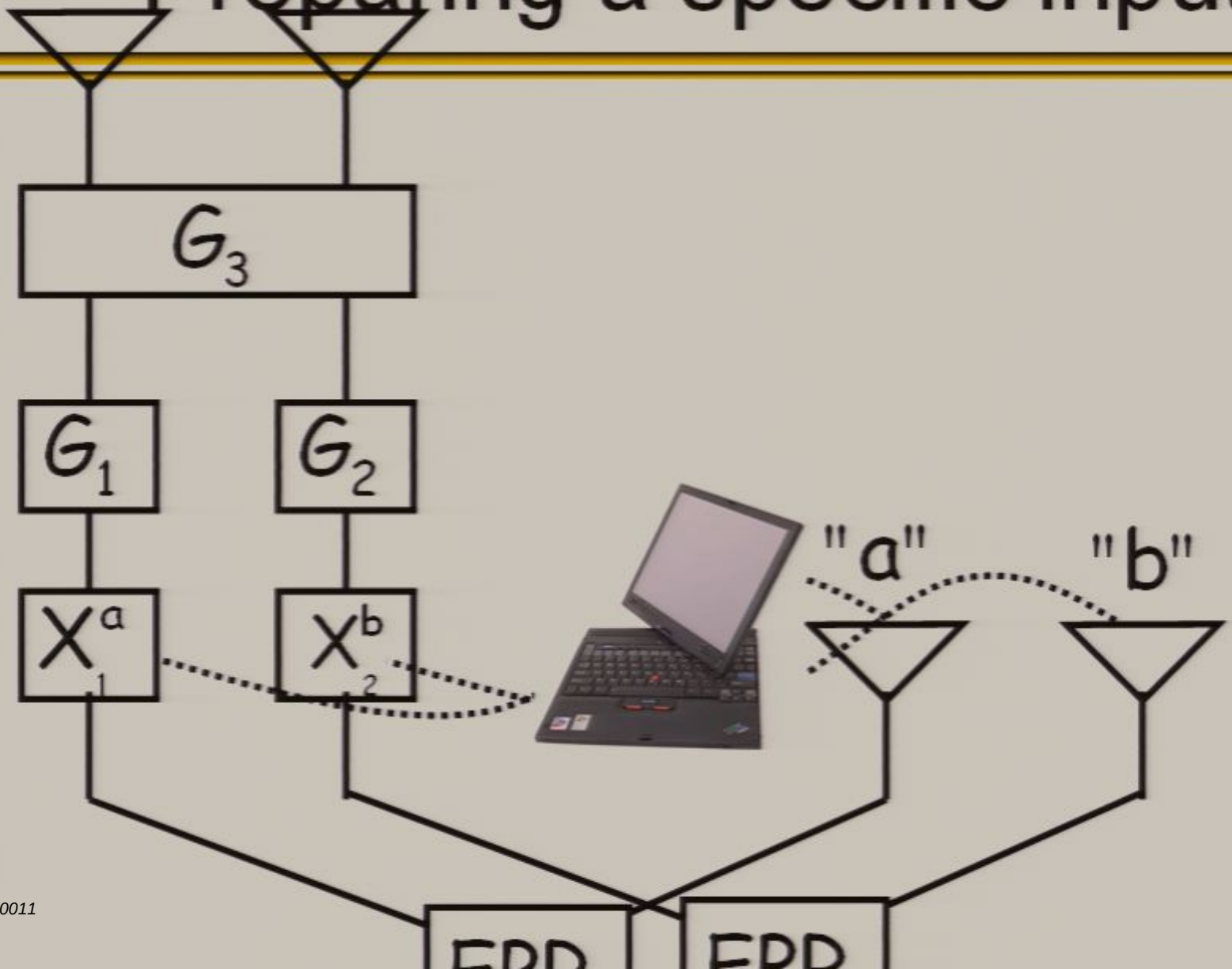
This procedure verifies the behaviour of the circuit, but how do we run it on a specific input?



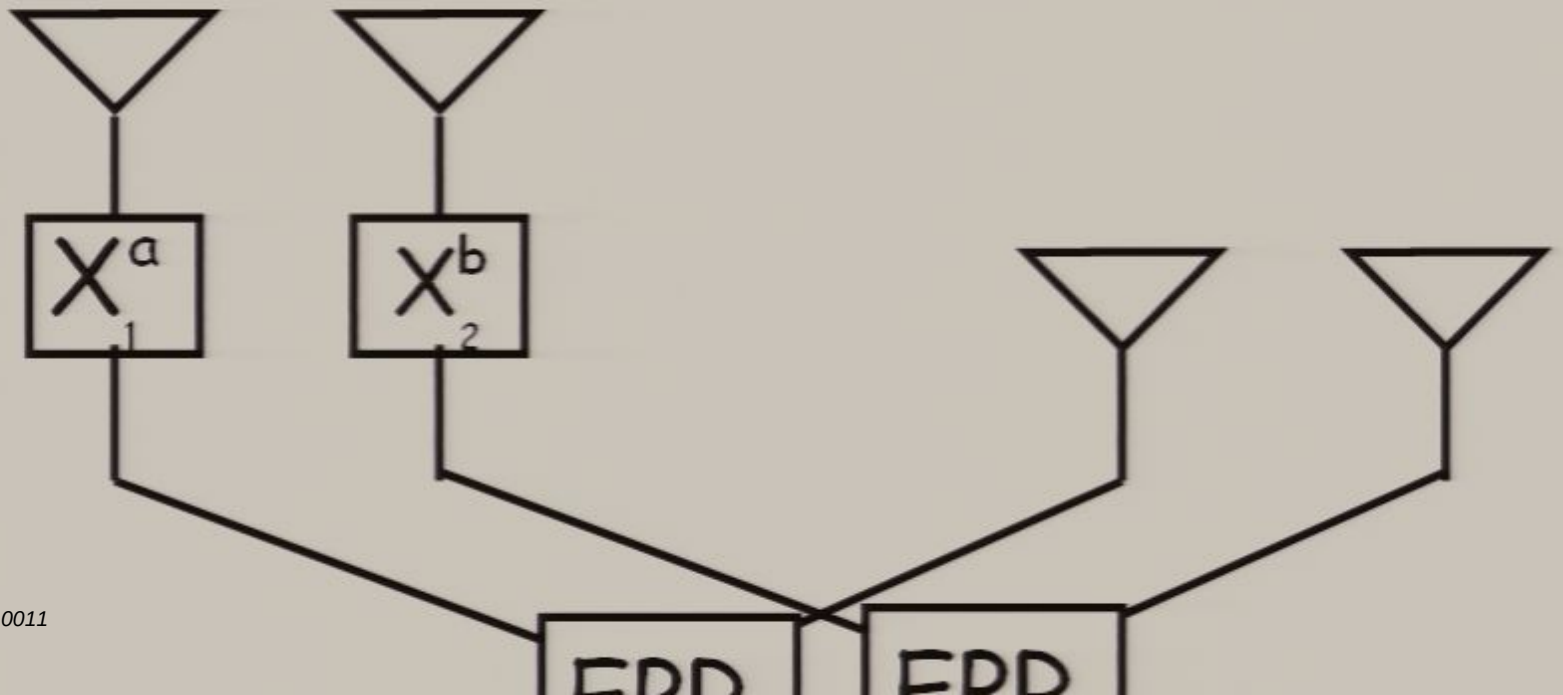
Preparing a specific input



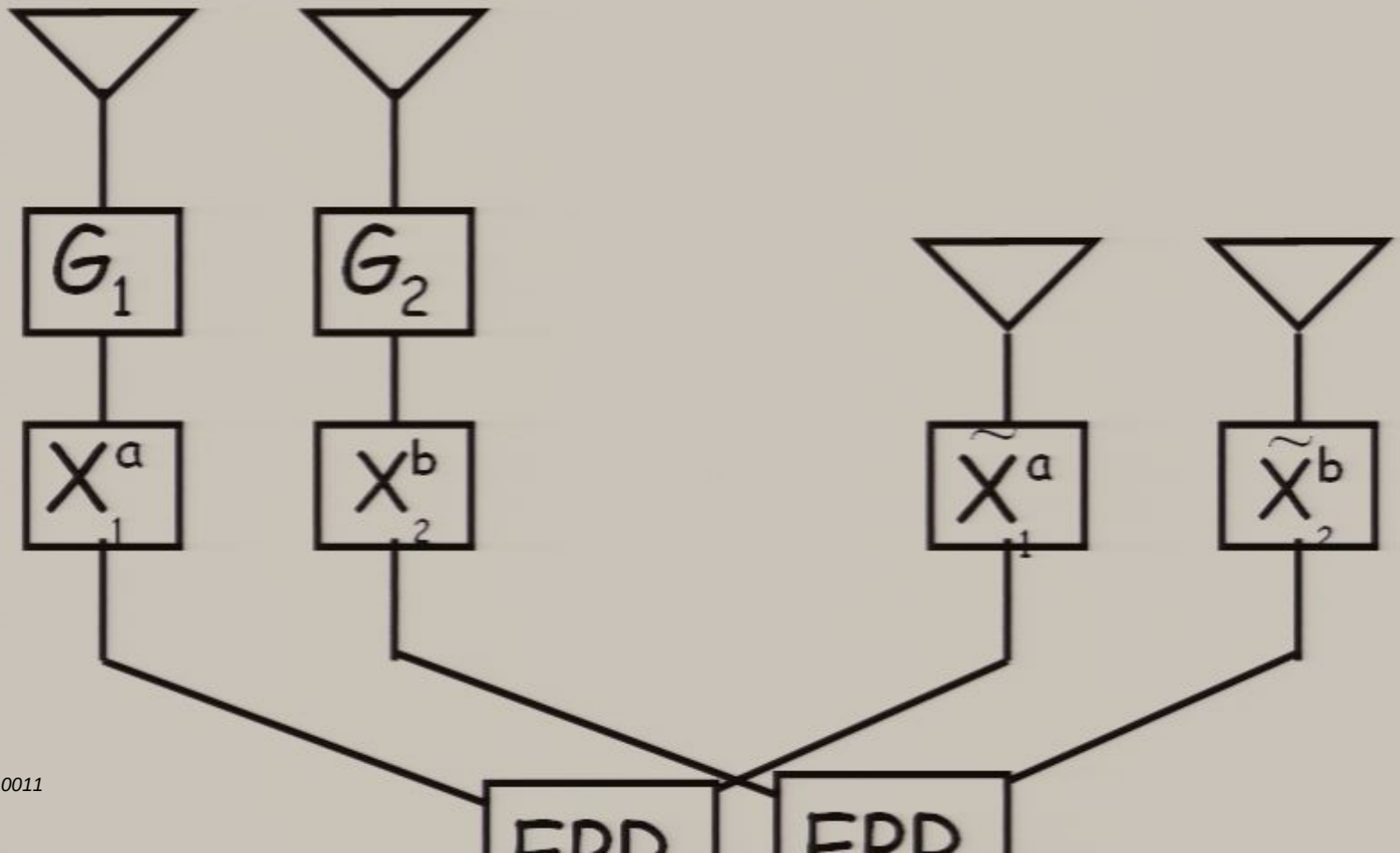
Preparing a specific input



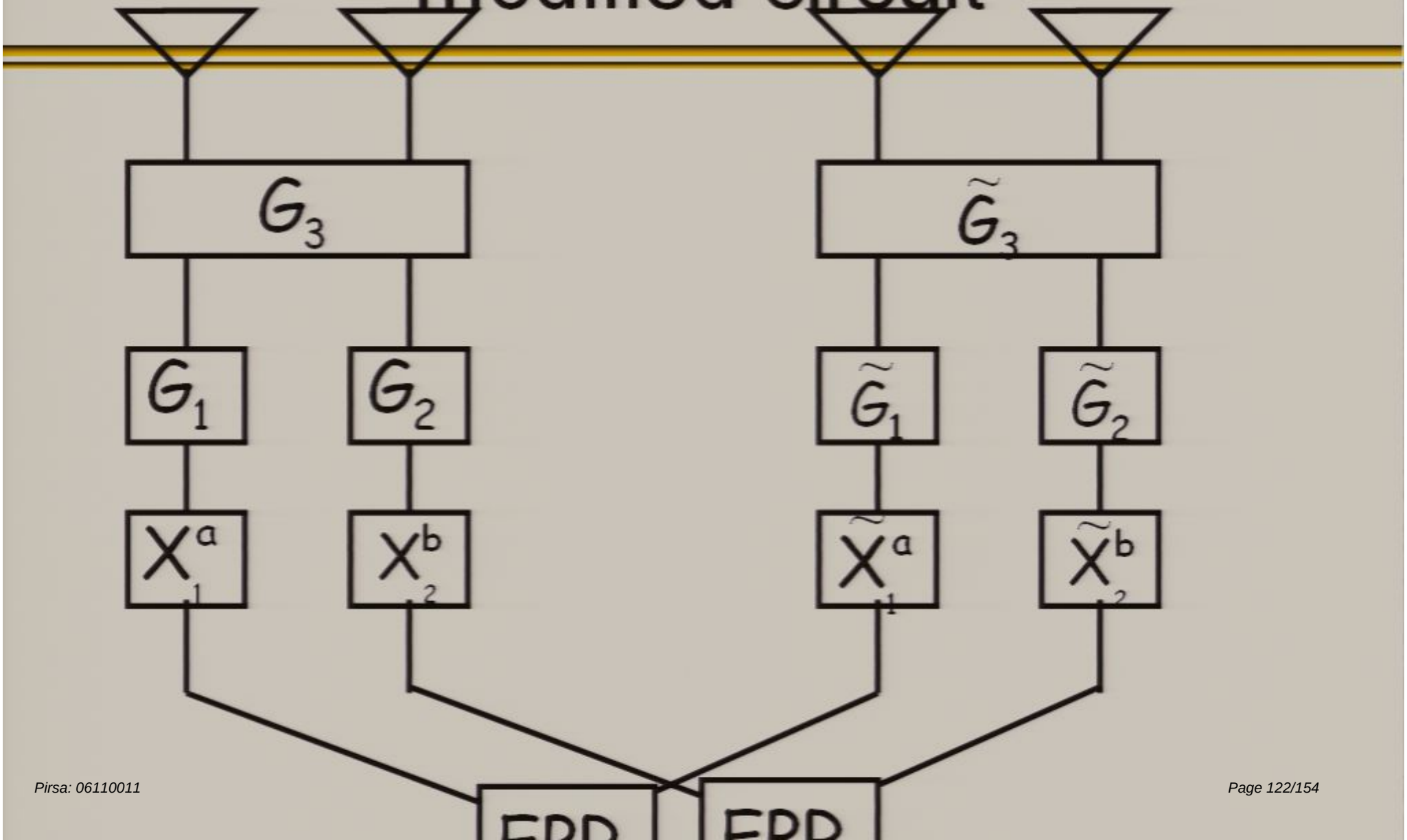
Then proceed to test this modified circuit



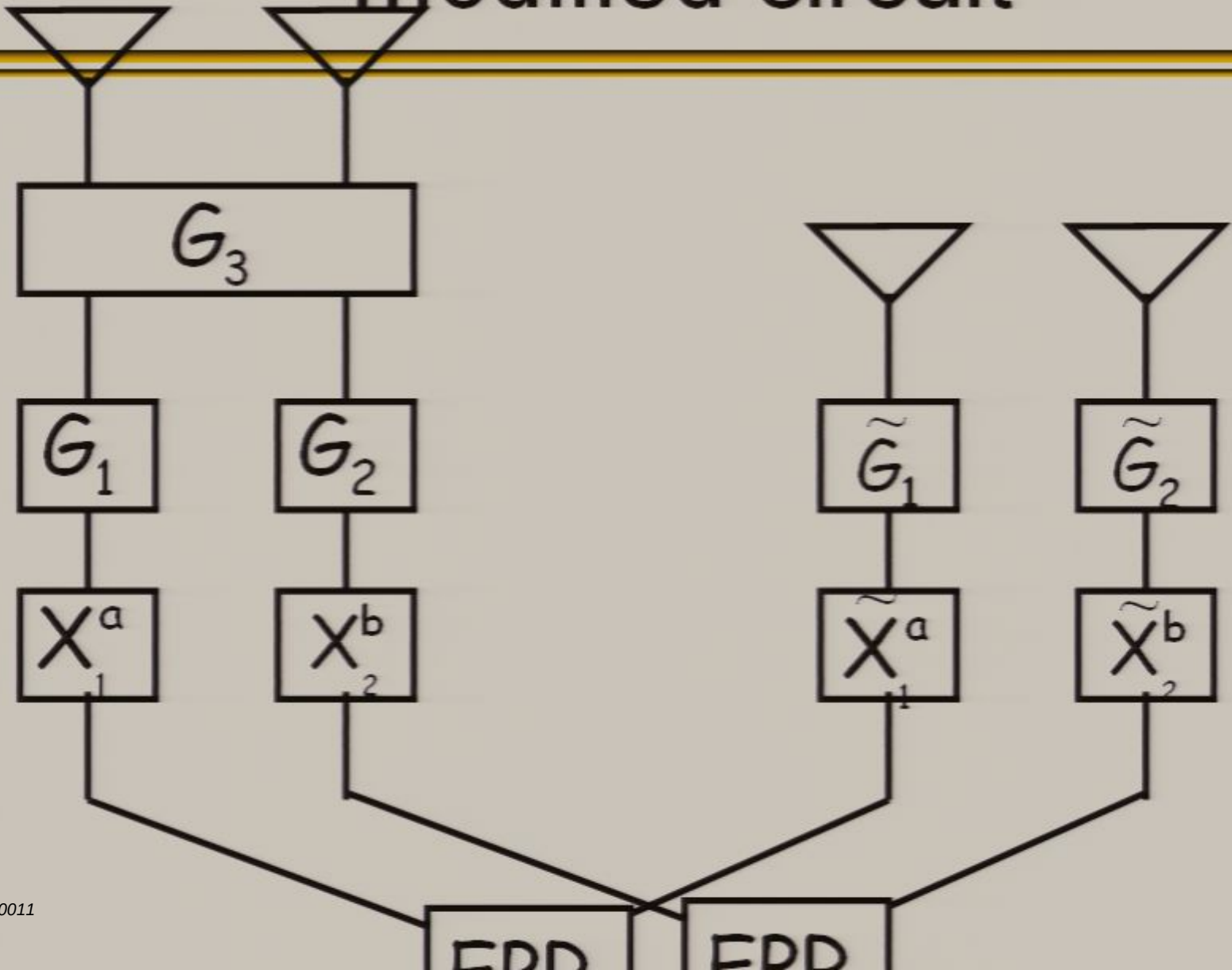
Then proceed to test this modified circuit



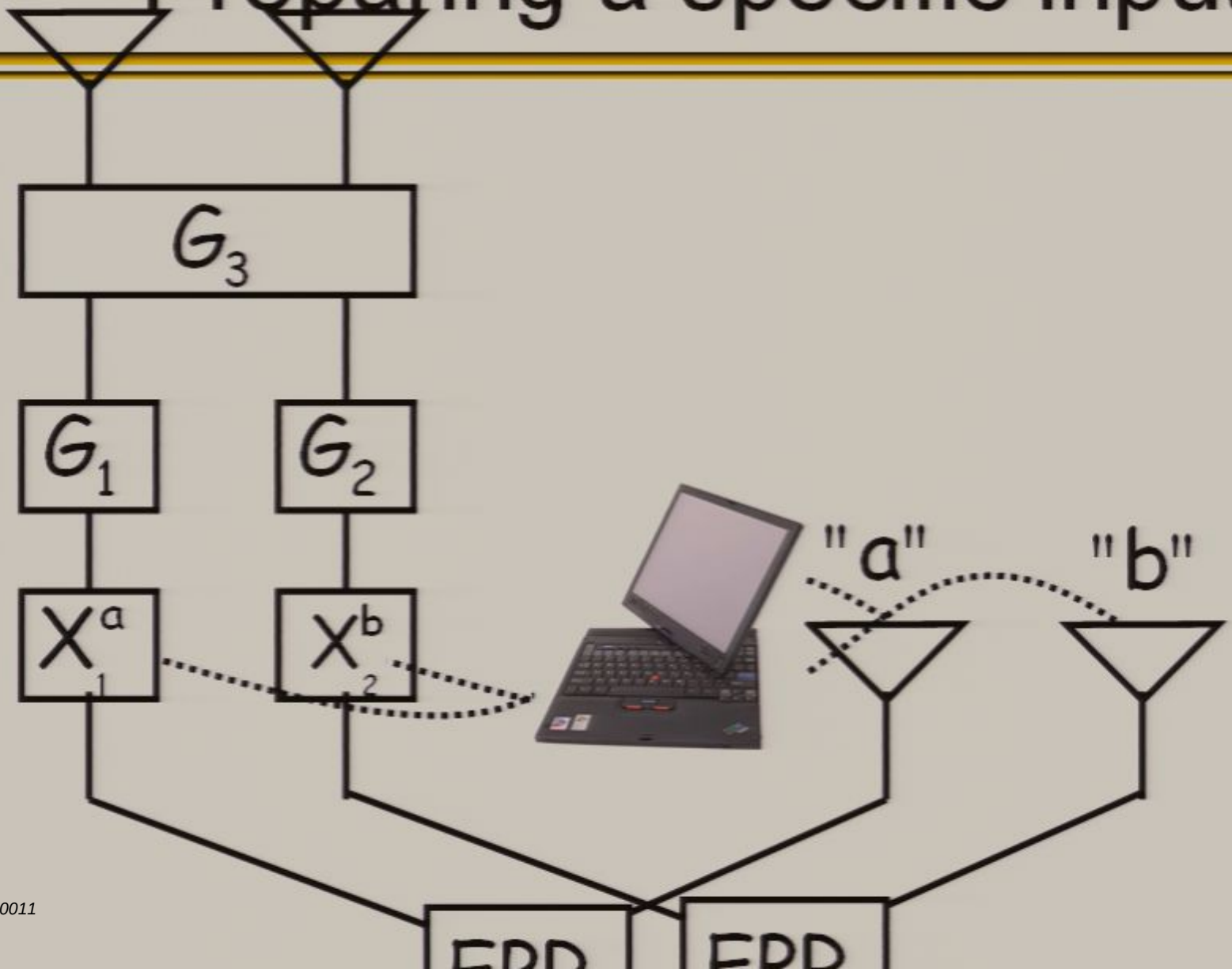
Then proceed to test this modified circuit



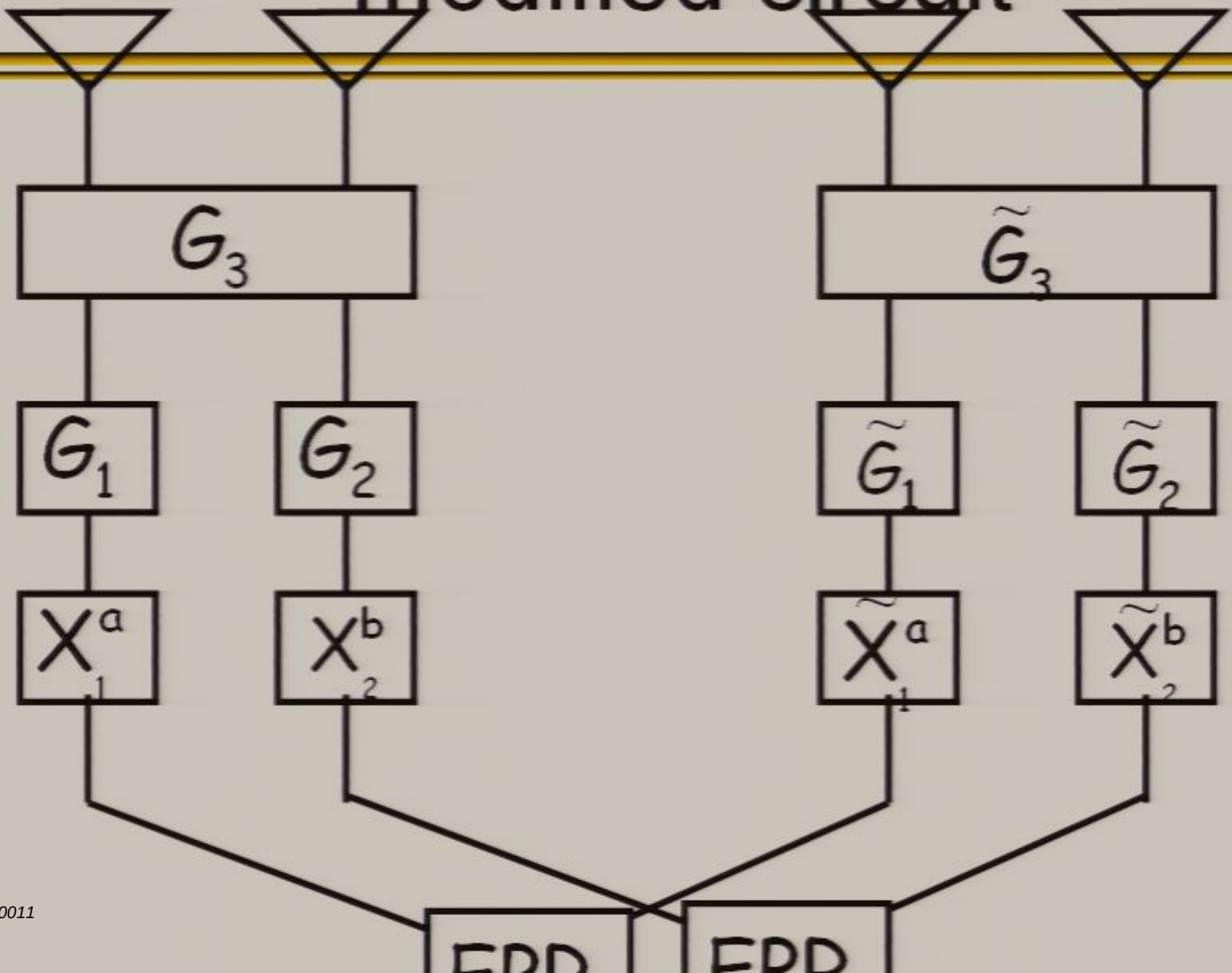
Then proceed to test this modified circuit



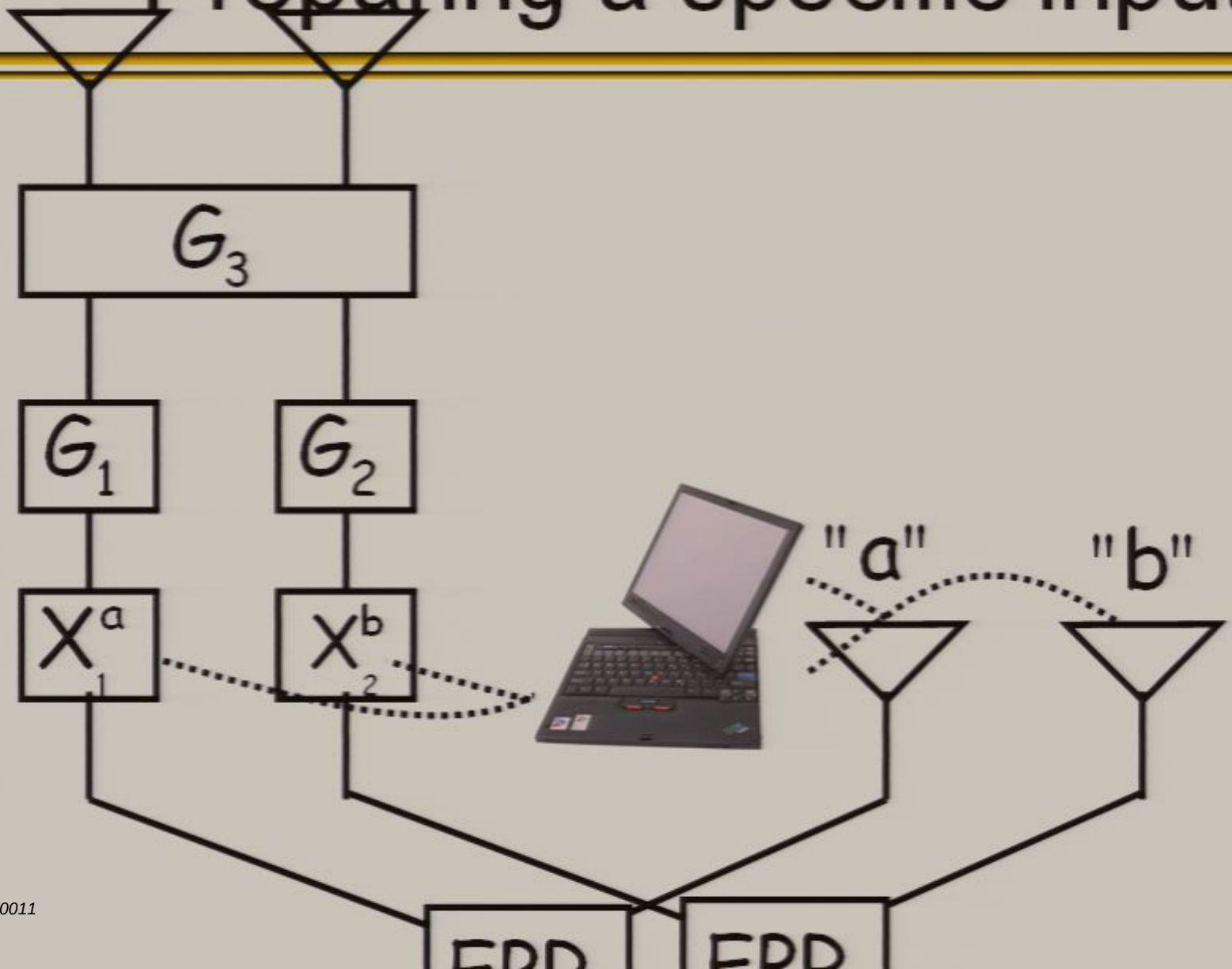
Preparing a specific input



Then proceed to test this modified circuit

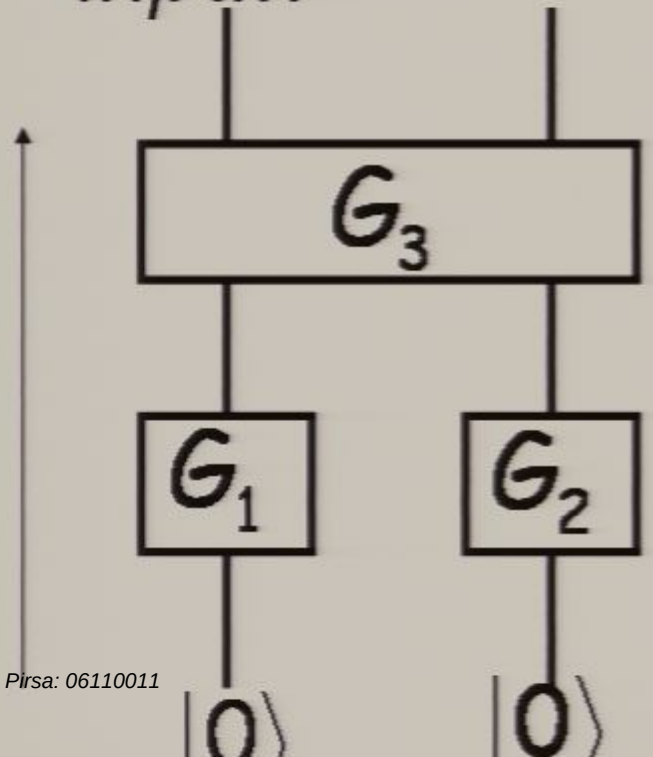


Preparing a specific input

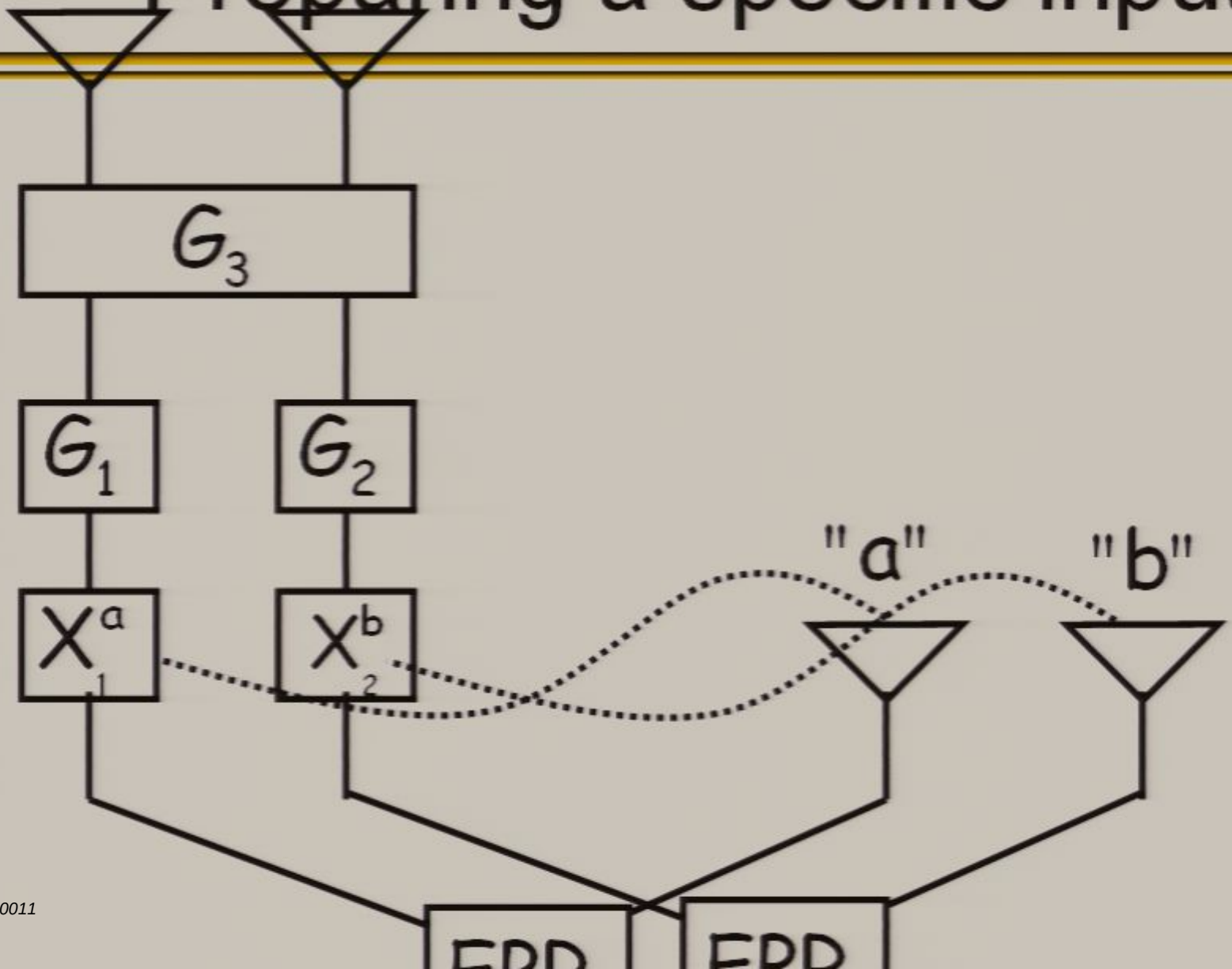


One last technical glitch

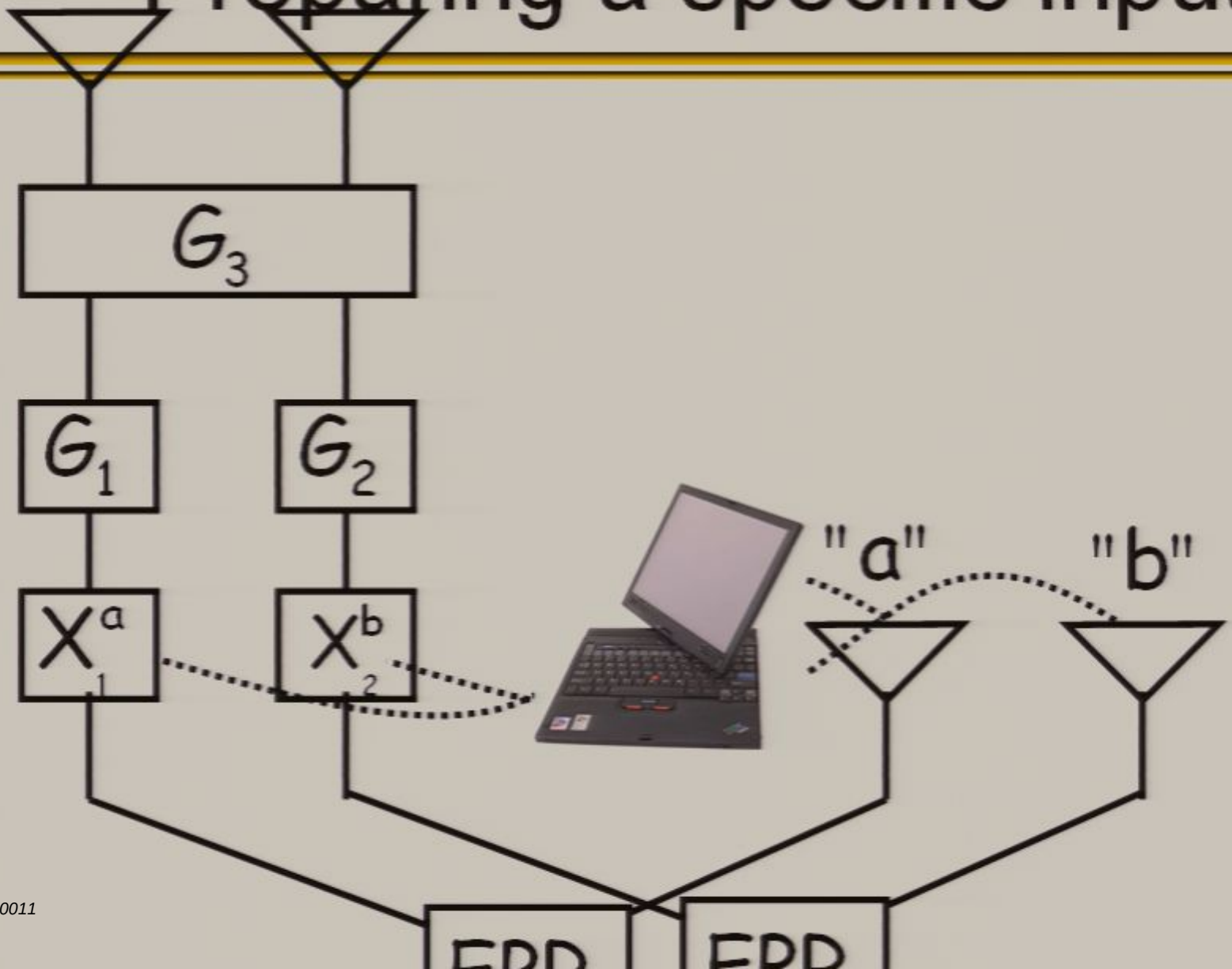
This procedure verifies the behaviour of the circuit, but how do we run it on a specific input?



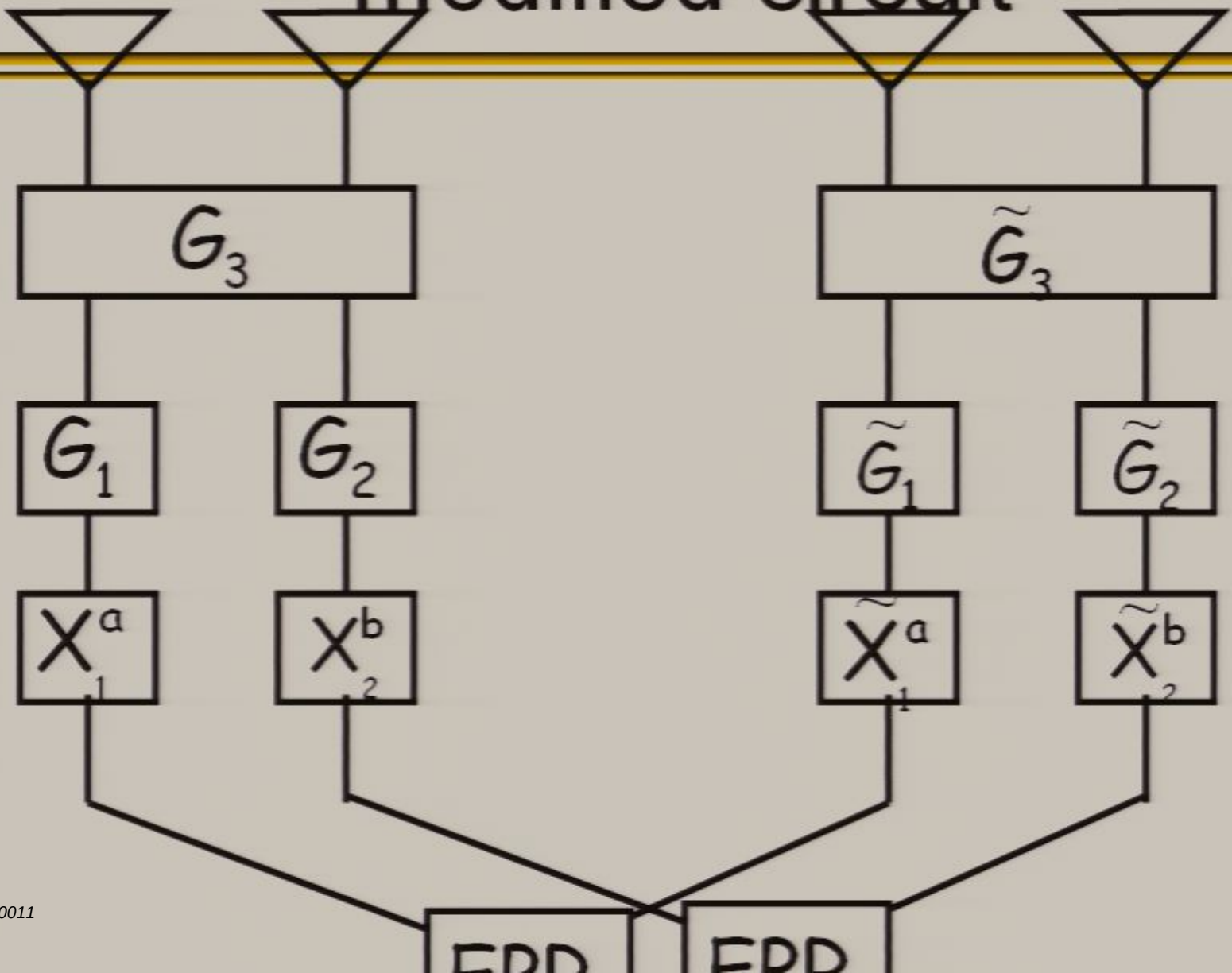
Preparing a specific input



Preparing a specific input

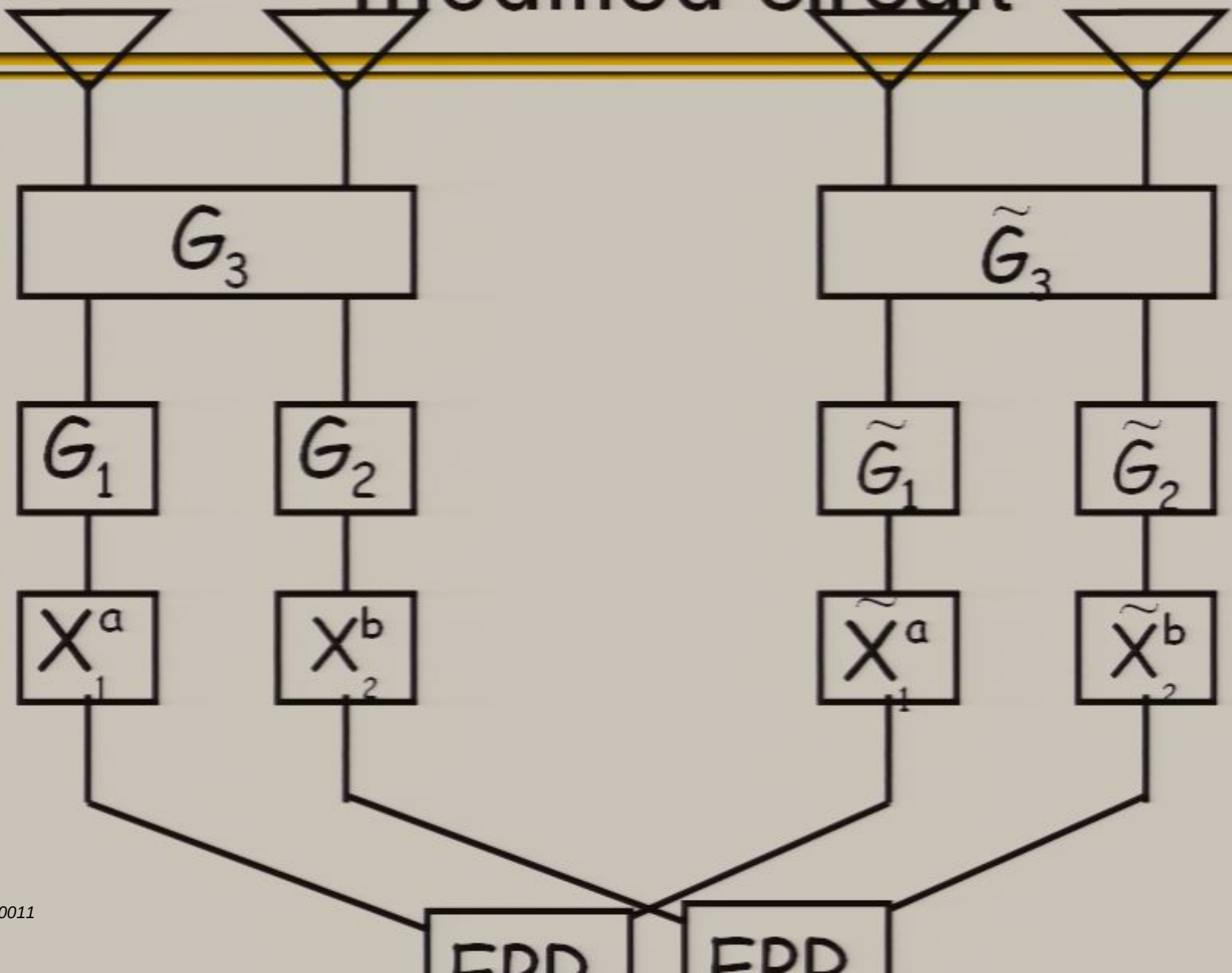


Then proceed to test this modified circuit



Some technical points

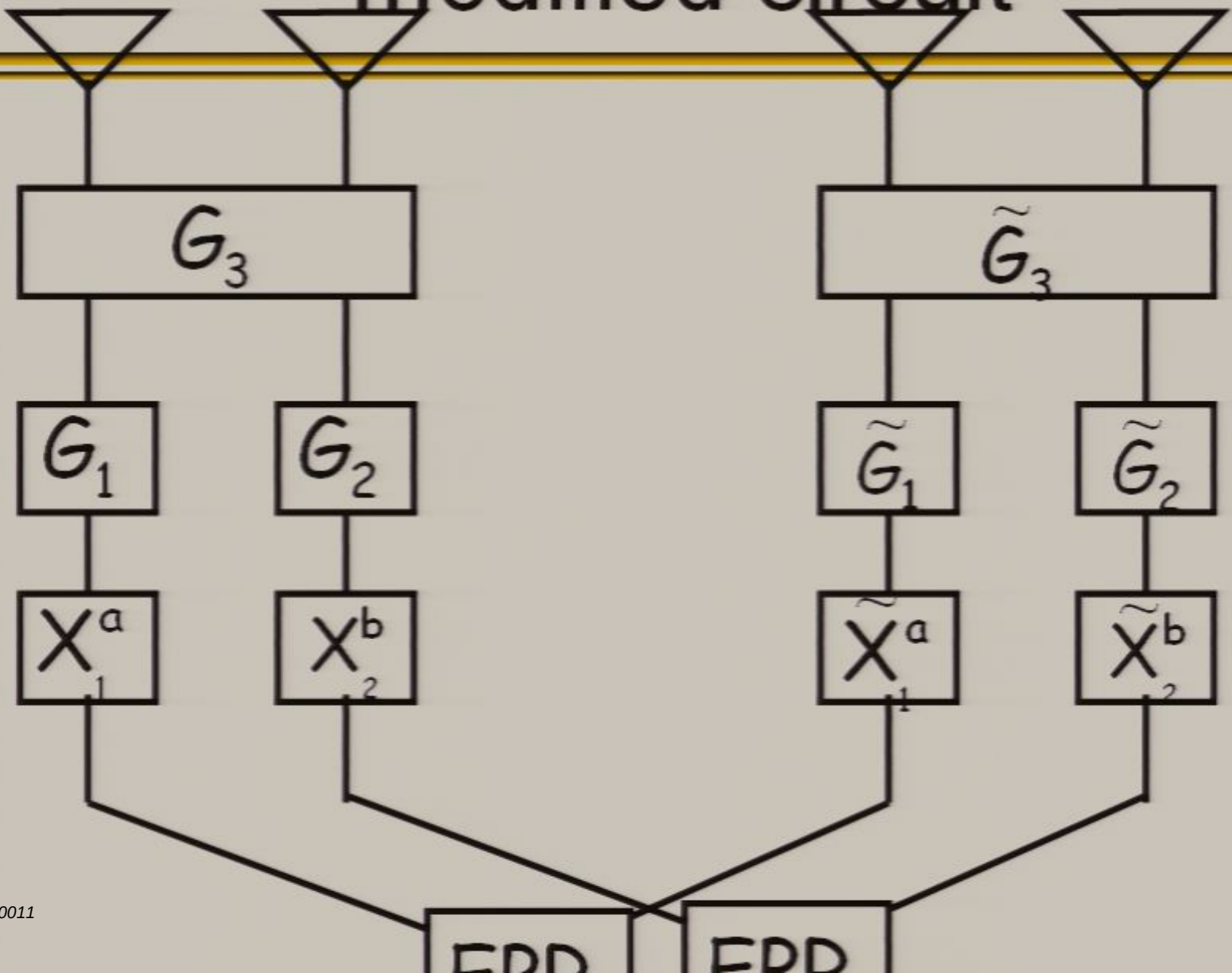
Then proceed to test this modified circuit



Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

Then proceed to test this modified circuit



Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

*NB We are not **assuming** that our gates or states only have real coefficients.*

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

*NB We are not **assuming** that our gates or states only have real coefficients.*

We are merely saying that we do not have a procedure in the case of non-real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

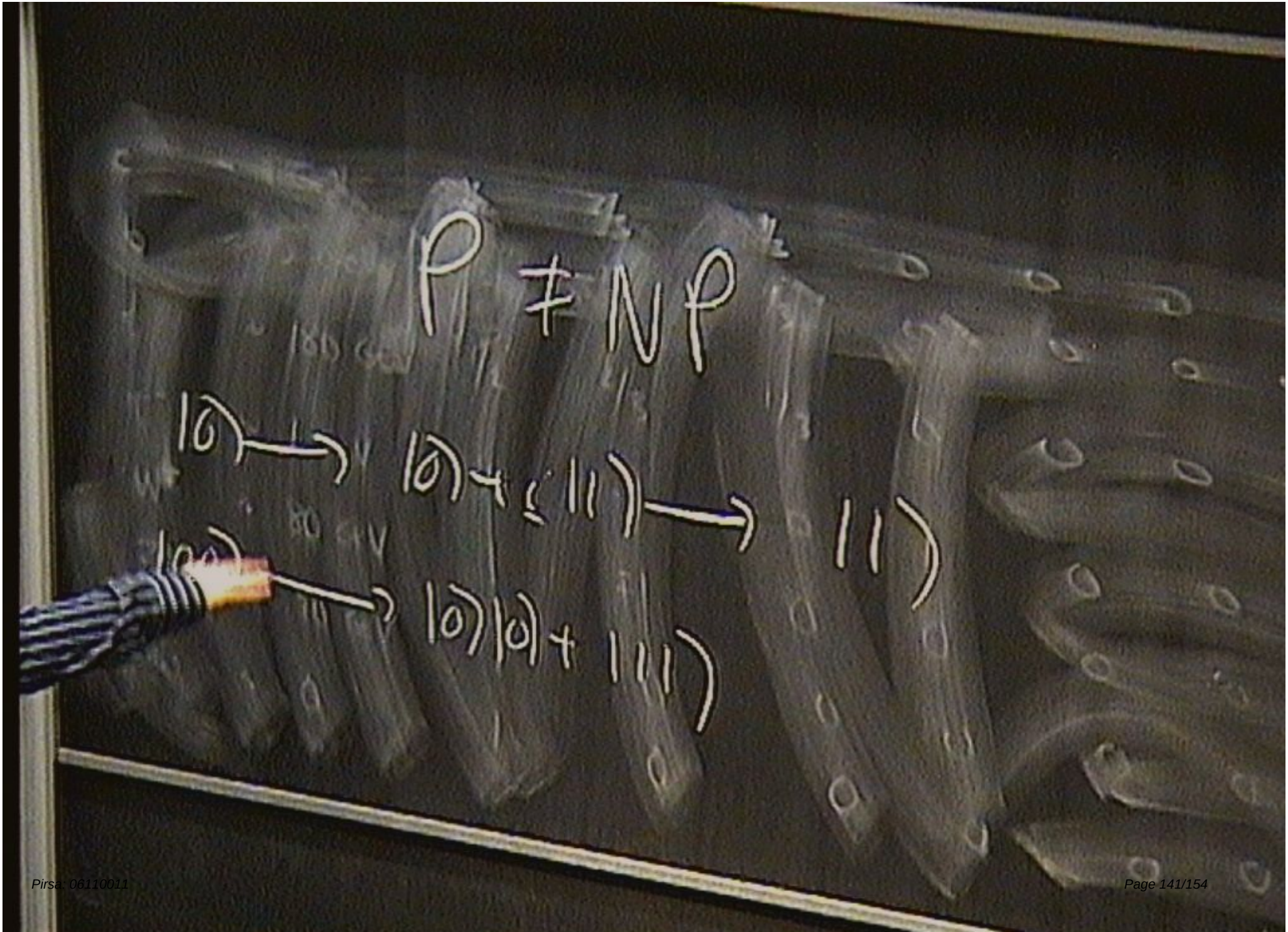
This is not for lack of trying. There is a fundamental reason for this:

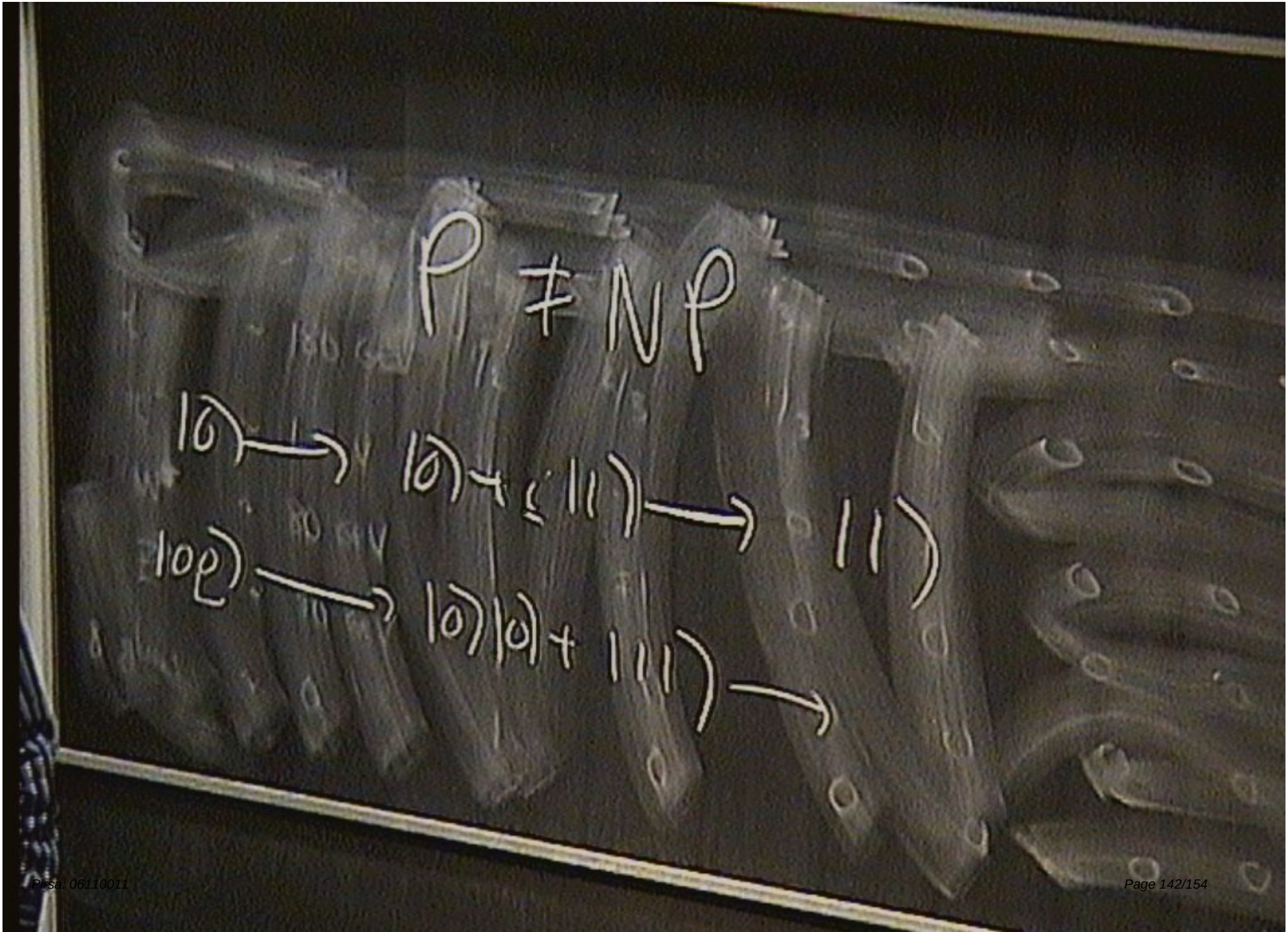
Some technical points

Our procedure is only good for verifying gates and states with real coefficients.

This is not for lack of trying. There is a fundamental reason for this:

1 complex bit can be simulated by 2 real bits (see e.g. Rudolph and Grover quant-ph/0210187). But the two systems are not "equivalent" according to our notion of equivalence. E.g. inner products are not


P ≠ NP
|0⟩ → |0⟩ + |1⟩ → |1⟩
|0⟩ → |0⟩|0⟩ + |1⟩


P ≠ NP
|0⟩ → |0⟩+ε|1⟩ → |1⟩
|0ρ⟩ → |0⟩|0⟩+|1⟩|1⟩ →

Precise statement of our main result

Let $T^1, T^2, \ldots, T^k \in U(2^n)$ *(acting on a constant number of qubits each)*

$x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0$

If $\mathrm{CircuitTest}(T^1, T^2, \ldots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

Precise statement of our main result

Let $T^1, T^2, \ldots, T^k \in U(2^n)$ *(acting on a constant number of qubits each)*

$x \in \{0,1\}^n, \varepsilon > 0, \gamma > 0$

If $\mathrm{CircuitTest}(T^1, T^2, \ldots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

Precise statement of our main result

If $\mathrm{CircuitTest}(T^1, T^2, \ldots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

The number of experiments is in $O\left(\frac{kn}{\varepsilon}\log\left(\frac{n}{\gamma}\right)\right)$

Precise statement of our main result

If $\mathrm{CircuitTest}(T^1, T^2, \cdots, T^k, x, \varepsilon, \gamma)$ *accepts, then with probability* $1 - O(\gamma)$ *the outcome probability distribution of the circuit is at total variation distance* $O((k+n)\varepsilon^{1/8})$ *from the distribution that comes from the measurement of* $T^k T^{k-1} \ldots T^2 T^1 |x\rangle$ *in the computational basis.*

The number of experiments is in $O\left(\frac{kn}{\varepsilon}\log\left(\frac{n}{\gamma}\right)\right)$

Some open problems and future directions

Some open problems and future directions

- *Apply these techniques to actual experiments. Modify as needed.*

Some open problems and future directions

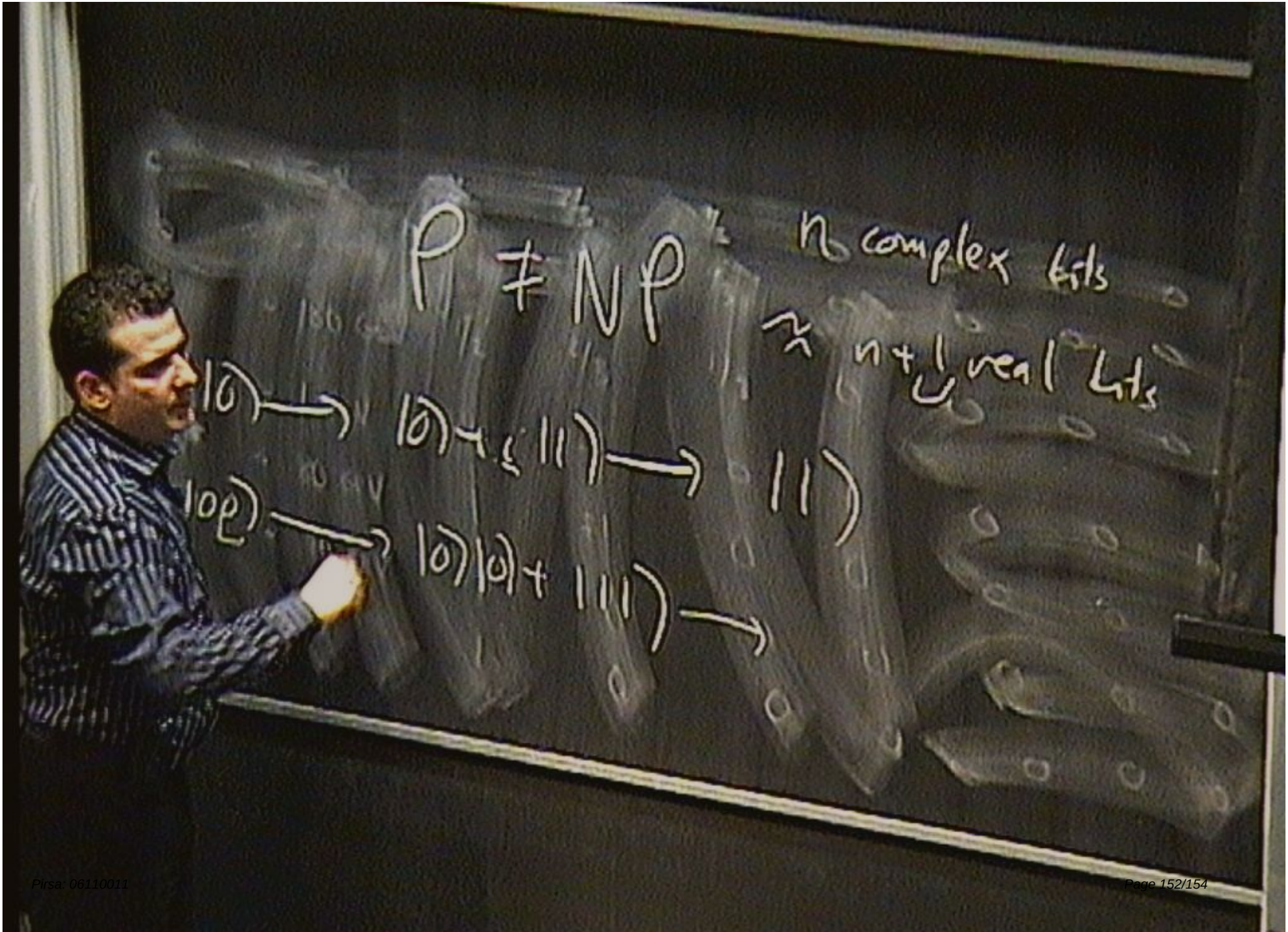
- *Apply these techniques to actual experiments. Modify as needed.*
- *Can we improve the asymptotics?*

Some open problems and future directions

- *Apply these techniques to actual experiments. Modify as needed.*
- *Can we improve the asymptotics?*
- *Can we add some other reasonable and testable assumptions that allow prepare-and-send QKD?*

Some open problems and future directions

- *Apply these techniques to actual experiments. Modify as needed.*
- *Can we improve the asymptotics?*
- *Can we add some other reasonable and testable assumptions that allow prepare-and-send QKD?*
- *Can something be done about the complex case?*


P ≠ NP
n complex bits
≈ n+1 real bits
|0⟩ → |0⟩+ε|1⟩ → |1⟩
|0ε⟩ → |0⟩|0⟩+|1⟩|1⟩ →

Some open problems and future directions

- *Apply these techniques to actual experiments. Modify as needed.*
- *Can we improve the asymptotics?*
- *Can we add some other reasonable and testable assumptions that allow prepare-and-send QKD?*
- *Can something be done about the complex case?*

The main assumptions of Mayers and Yao are

1) *Locality (i.e. measurements at A commute with those at B)*
2) *Repeatability of experiments*
3) *Trusted classical apparatus*

However, the results are not "robust". The results hold exactly if the statistics are satisfied exactly.

Any realistic application will need to be robust.

(Assuming robustness) This might be the only way, using only these assumptions, to verifiably securely