A crash course on Quantum Information and Quantum Cryptography

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.

A crash course on Quantum Information and some examples for Quantum Cryptography

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.

A crash course on Quantum Information and some examples for Quantum Cryptography
... If there’s time

Ricardo Faleiro, IT-Aveiro

13/11/24

This project was funded within the DIGITAL-2021-QCI-01 Programme that has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No. 101091730.

2/24/70/1

Quantum Information Theory

False

Conversation w/ Steve Wiesner, who told me that:

A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacity of one bit, two bits of information; subject however to the constraint that, ~~the receiver may at his choice read either~~ whichever bit the receiver chooses to read, the other bit is destroyed.

2/24/70 | 1 Quantum Information Theory False

Conversation w/ Steve Wiesner, who told me that:

A variation on the Einstein-Rosen-Podolsky Gedankenexperiment can be used to send, through a channel with a nominal capacit[y] … bits of information; subject howev[er] … ~~the receiver may~~ … whichever bit the ~~reader~~ receiv[er] … the other bit is destroyed.

This paper treats a class of codes made possible by restrictions on measurement related to the uncertainty principal. Two concrete examples and some general results are given.

Conjugate Coding *

Stephen Wiesner

Columbia University, New York, N.Y.
Department of Physics

	Quantum Mechanics	Quantum Information Theory

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be "real"	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.

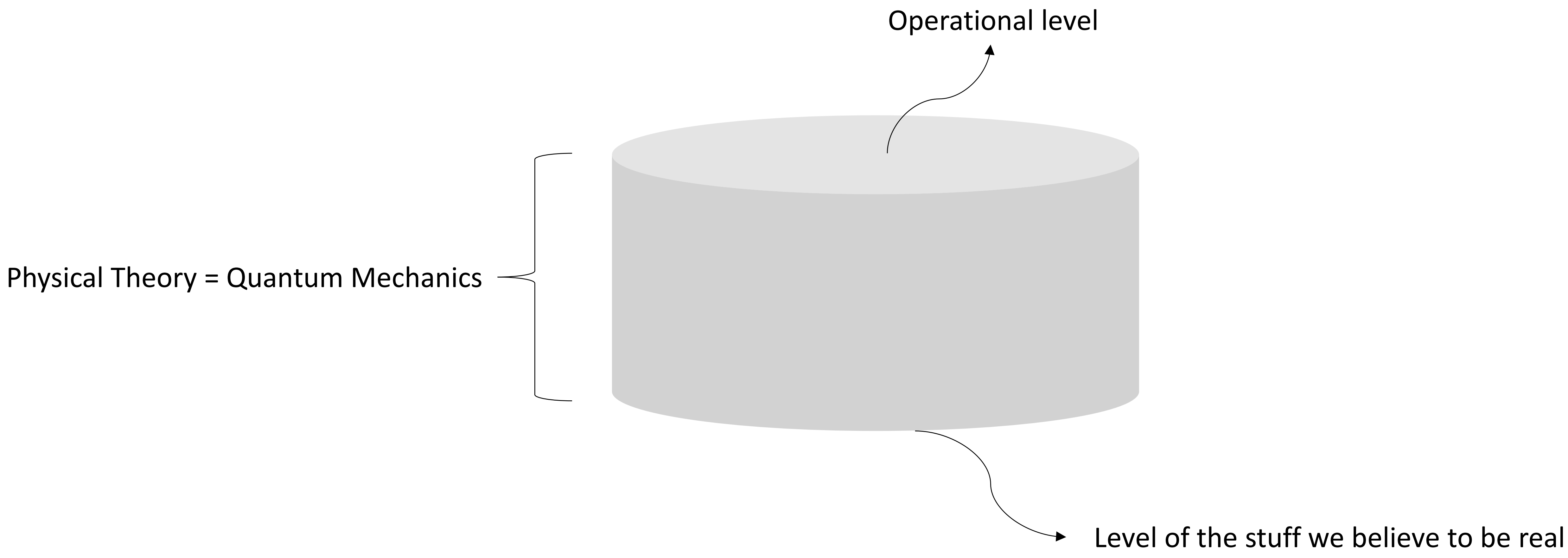
	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be "real"	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.
Philosophical stance	Physical theory; Abides implicitly to physicalism;	

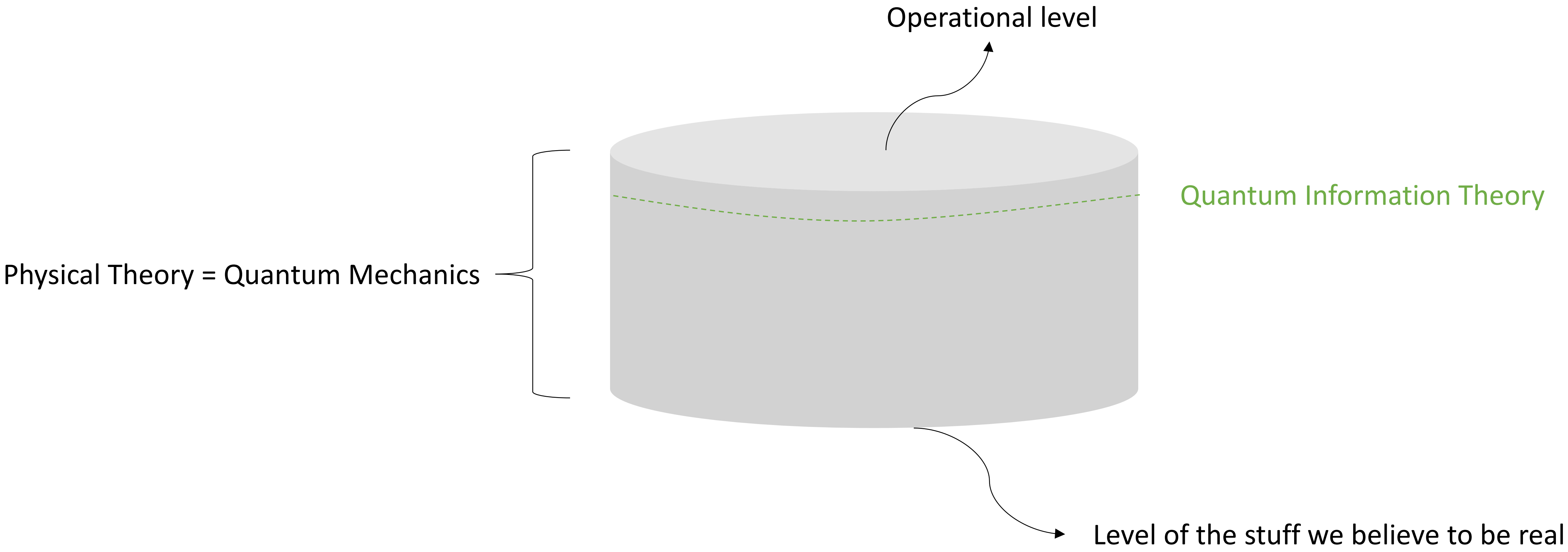
	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be "real"	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.
Philosophical stance	Physical theory; Abides implicitly to physicalism;	Informational theoretic framework; Instrumental;

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.
Philosophical stance	Physical theory; Abides implicitly to physicalism;	Informational theoretic framework; Instrumental;
Goals	Understanding and predicting physical phenomena (e.g., atomic structures, scattering processes, decays).	

	Quantum Mechanics	Quantum Information Theory
Important Concepts	Particles; Fields; Spins, Momentum; Energy (Hamiltonians) i.e Physical stuff that are believed to be “real”	Probabilities; Entropies; Correlations; Mutual Information i.e Information that as agents/experimenters we care to know
States and evolution	Wave functions of physical systems represented in continuous basis of space or momenta, evolving according to the Schroedinger equation.	State vectors or density matrices of finite dimensional registers of abstract systems, evolving discretely with unitary operators.
Philosophical stance	Physical theory; Abides implicitly to physicalism;	Informational theoretic framework; Instrumental;
Goals	Understanding and predicting physical phenomena (e.g., atomic structures, scattering processes, decays).	Manipulating and processing information, often for tasks like quantum computing, communication, and cryptography

Physical Theory = Quantum Mechanics


Operational level
Physical Theory = Quantum Mechanics
Level of the stuff we believe to be real


Operational level
Quantum Information Theory
Physical Theory = Quantum Mechanics
Level of the stuff we believe to be real

“But if quantum mechanics isn’t physics in the usual sense — if it’s not about matter, or energy, or waves, or particles — then what is it about? From my perspective, it’s about information and probabilities and observables, and how they relate to each other.” – Scott Aaronson, Quantum Computing Since Democritus

"But if quantum mechanics isn't physics in the usual sense — if it's not about matter, or energy, or waves, or particles — then what is it about? From my perspective, it's about information and probabilities and observables, and how they relate to each other." – Scott Aaronson, Quantum Computing Since Democritus

So what is different? The theory is the same, but taken from a new perspective:

"But if quantum mechanics isn't physics in the usual sense — if it's not about matter, or energy, or waves, or particles — then what is it about? From my perspective, it's about information and probabilities and observables, and how they relate to each other." – Scott Aaronson, Quantum Computing Since Democritus

So what is different? The theory is the same, but taken from a new perspective:

- **QM is a physical theory grounded in a notion of physicalism, that is, it focuses on "real" physical systems and their properties;**

- **QI is an epistemic framework concerned with studying the manipulation and processing of information emergent from the quantum mechanical phenomena**.

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

E.g. Typically, one tries to be as agnostic as possible about the contents of the boxes, but sometimes general assumptions can be established. For instance, we may consider preparations that only output states up to a certain dimension or energy.

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

Going from QM to QI some aspects of the phenomenology of quantum mechanics which were consider troubling can be promoted to resources for information processing:

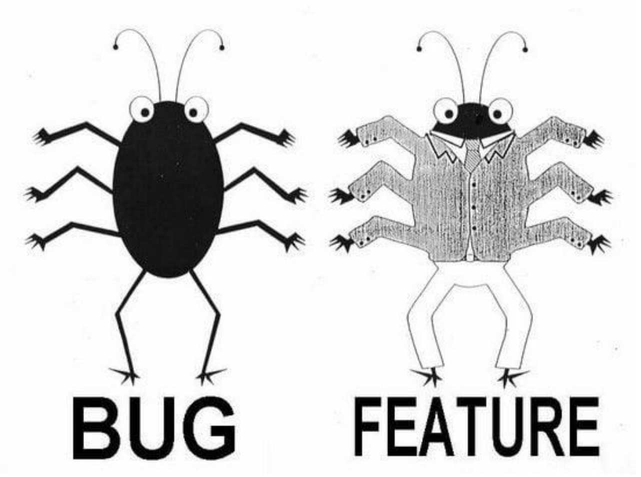
- Coherence, superposition;
- Measurement incompatibility;
- Entanglement;
- Nonlocality

It will be useful then to conceptualize Quantum information as a theory of processes s.t:

- We don’t really care about the inner workings of the processes/boxes in great detail;
- We have a good understanding of how the boxes behave, with respect their inputs/outputs, such that, we can model them within the formalism of quantum mechanics consistently with the observed behavior of the boxes;

Going from QM to QI some aspects of the phenomenology of quantum mechanics which were consider troubling can be promoted to resources for information processing:

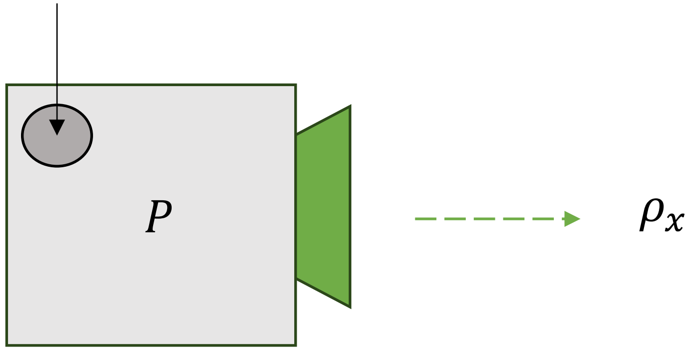
- Coherence, superposition;
- Measurement incompatibility;
- Entanglement;
- Nonlocality



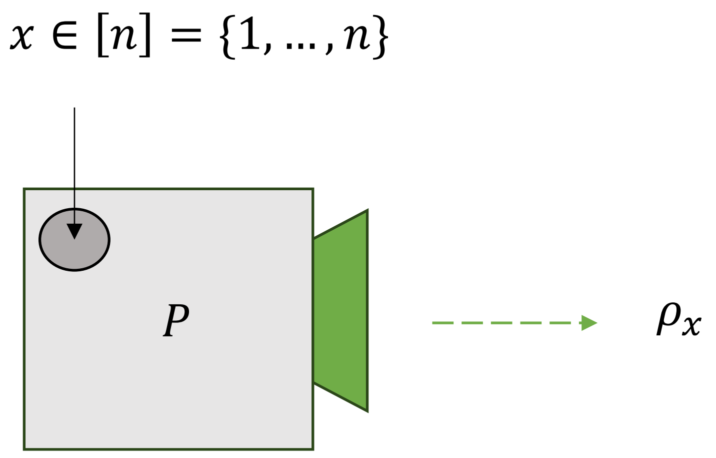
(Deterministic) Preparations

(Deterministic) Preparations

$x \in [n] = \{1, \dots, n\}$

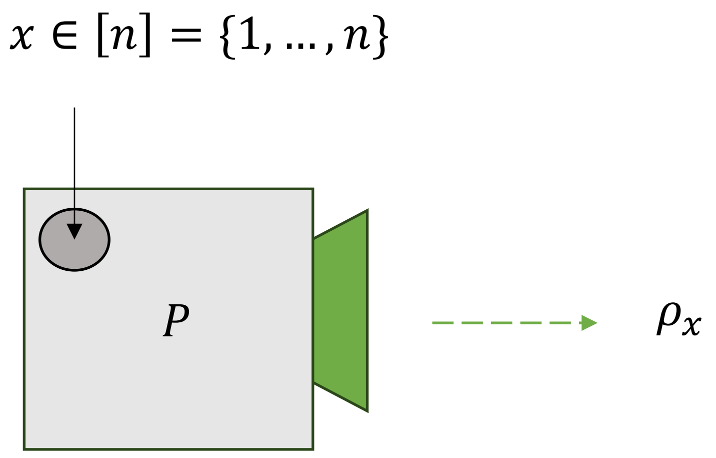


(Deterministic) Preparations



In the lab it might look more like this…

(Deterministic) Preparations



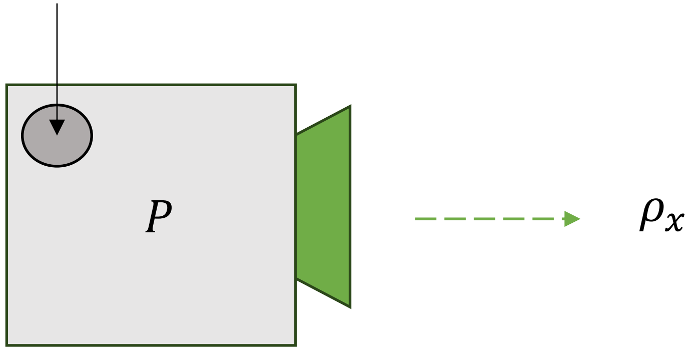
In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\rho_x | \, x \in [n]\} \rangle$
  - $\boldsymbol{H}$ = Hilbert space

(For finite dimension, can be assumed to be a complex Euclidean space. A linear (vector) field with the Euclidean metric and usual inner product of vectors in $\mathbb{C}^n$, where the vectors, operators etc, can have over complex numbers as components.)

(Deterministic) Preparations

$x \in [n] = \{1, \ldots, n\}$



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\rho_x | \, x \in [n]\}\rangle$
  - $\boldsymbol{H}$ = Hilbert space

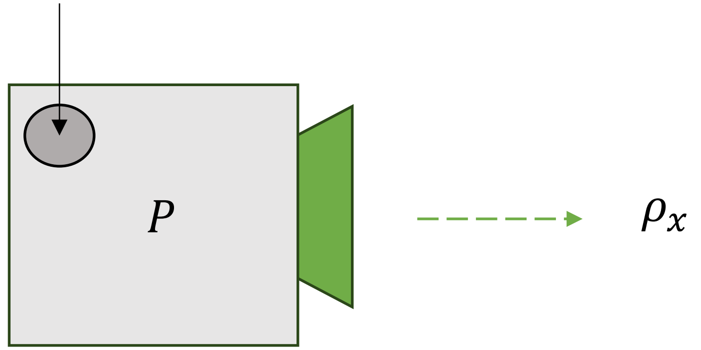
(For finite dimension, can be assumed to be a complex Euclidean space. A linear (vector) field with the Euclidean metric and usual inner product of vectors in $\mathbb{C}^n$, where the vectors, operators etc, can have over complex numbers as components.)

  - $\{\rho_x | \, x \in [n]\} = \{\rho_1, \rho_2, \ldots, \rho_n\}$

Each ρ_x is called a ***density operator***. They are, positive semi-definite, trace one, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

(Deterministic) Preparations

$x \in [n] = \{1, \dots, n\}$



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\rho_x | \, x \in [n]\} \rangle$
  - $\boldsymbol{H}$ = Hilbert space

(For finite dimension, can be assumed to be a complex Euclidean space. A linear (vector) field with the Euclidean metric and usual inner product of vectors in $\mathbb{C}^n$, where the vectors, operators etc, can have over complex numbers as components.)

  - $\{\rho_x | \, x \in [n]\} = \{\rho_1, \rho_2, \dots, \rho_n\}$

Each ρ_x is called a ***density operator***. They are, positive semi-definite, trace one, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Hermiticity: $\rho_x = \rho_x^\dagger$

Positive Semi-Definiteness: For any vector $| \psi \rangle \in \boldsymbol{H}$, we have $\langle \psi | \rho | \psi \rangle \geq 0$. Equivalent to say that the spectrum, the set of eigenvalues, is non-negative.

Trace Condition: $Tr(\rho) = 1$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$\downarrow$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Second, define the density operators for the possible inputs:

- $\{\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|, \rho_3 = |+\rangle\langle +|, \rho_4 = |-\rangle\langle -|\}$

Where,
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

Second, define the density operators for the possible inputs:

- $\{\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|, \rho_3 = |+\rangle\langle +|, \rho_4 = |-\rangle\langle -|\}$

Where,

- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$\{|0\rangle\langle 0| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, |1\rangle\langle 1| = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix},$

$|+\rangle\langle +| = \begin{pmatrix}1/2 & 1/2\\1/2 & 1/2\end{pmatrix}, \; |-\rangle\langle -| = \begin{pmatrix}1/2 & -1/2\\-1/2 & 1/2\end{pmatrix}\},$

Special case, where the density operators are outer products of a single vectors. These are called pure state.

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Second, define the density operators for the possible inputs:

- $\{\rho_1 = |0\rangle\langle 0|, \rho_2 = |1\rangle\langle 1|, \rho_3 = |+\rangle\langle +|, \rho_4 = |-\rangle\langle -|\}$

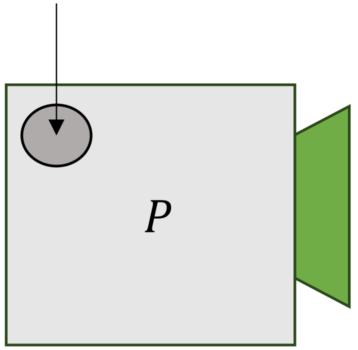
Where,
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$\{|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$

$|+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, \ |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\},$

Special case, where the density operators are outer products of a single vectors. These are called pure state.

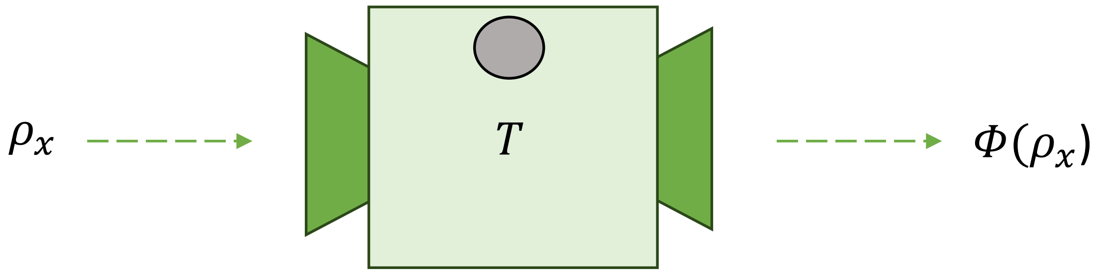
$x = 3$



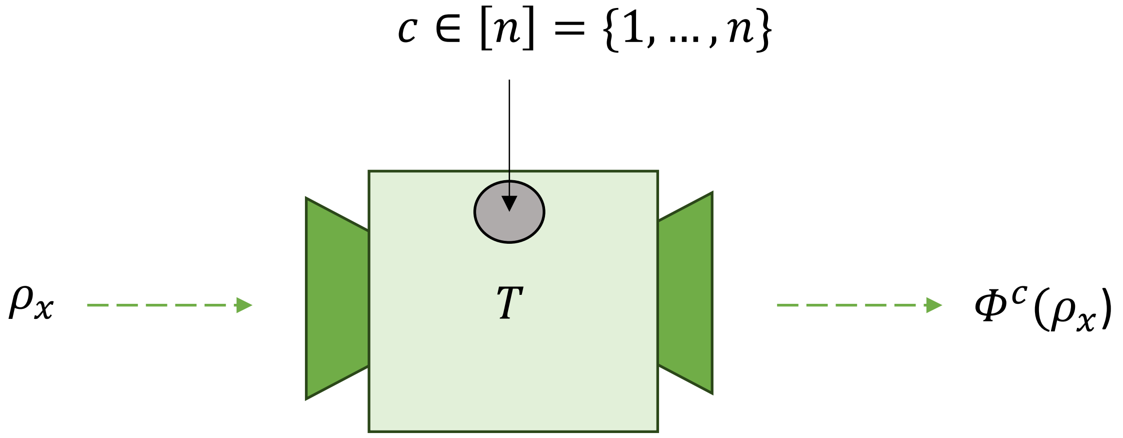
$| +\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Transformations

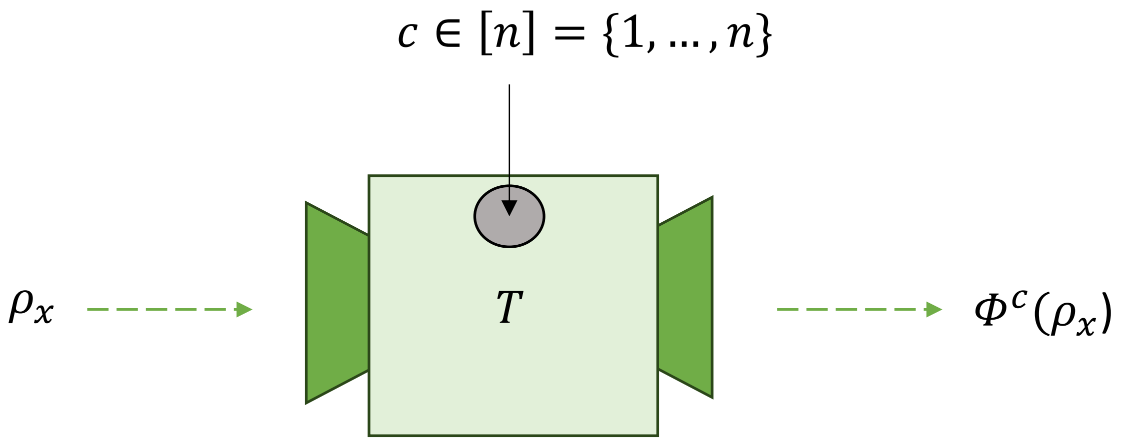
Transformations



(Control-)Transformations

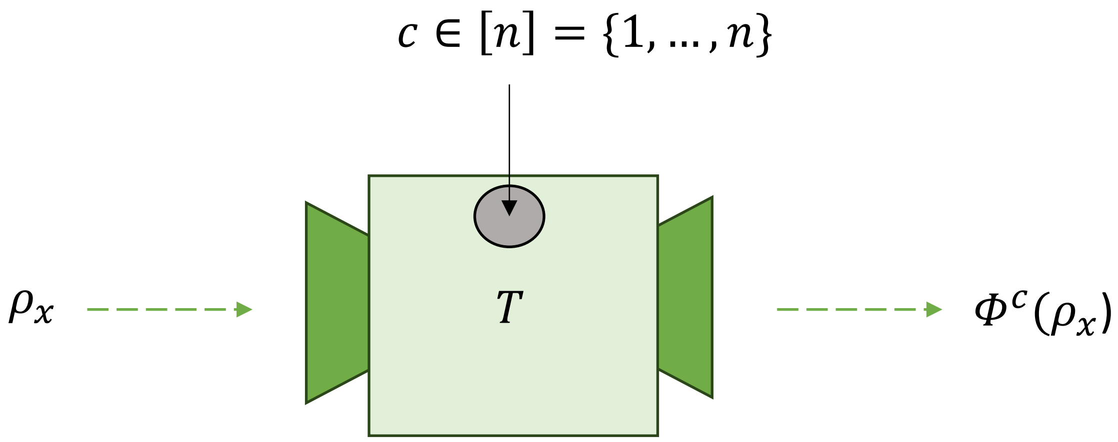


(Control-)Transformations



In the lab it might look more like this…

(Control-)Transformations



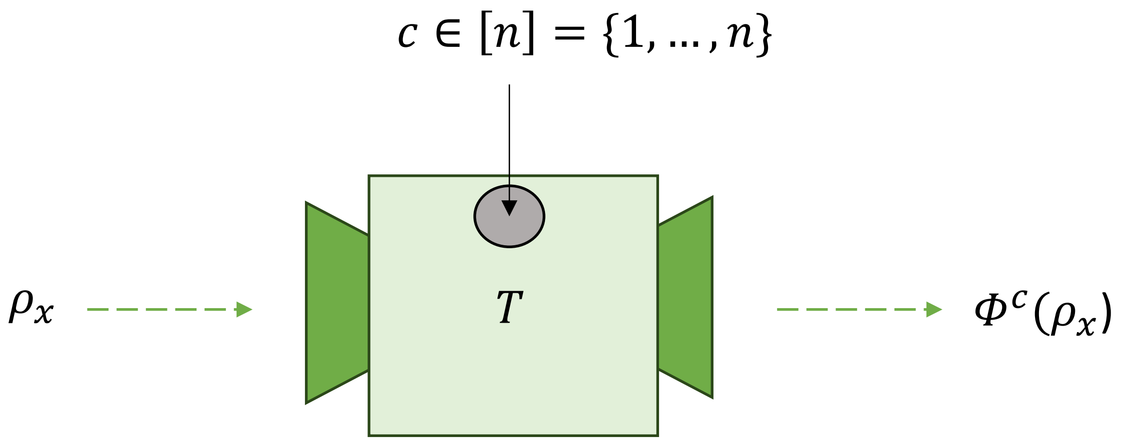
In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\Phi^c\}_c \rangle$

A transformation is described by a Completely-Positive-Trace-Preserving (CPTP) Map

$$\forall_c\, \Phi^c : \boldsymbol{H} \to \boldsymbol{H}$$

(Control-)Transformations



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\Phi^c\}_c \rangle$

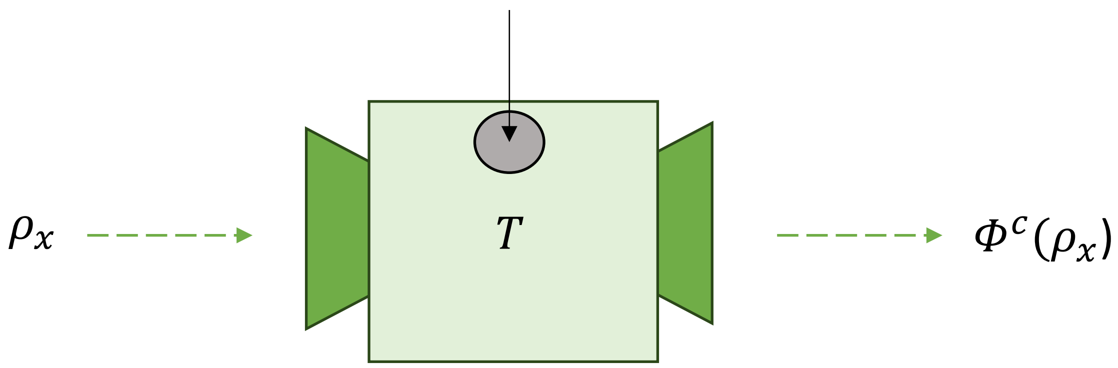
A transformation is described by a Completely-Positive-Trace-Preserving (CPTP) Map

$$\forall_c \; \Phi^c : \boldsymbol{H} \to \boldsymbol{H}$$

In the Kraus representation $\forall_c \; \Phi^c \Leftrightarrow \{K_i\}^c$

- $\Phi^c(\rho_x) = \sum_i K_i^c \rho_x K_i^{c\,\dagger}$

(Control-)Transformations



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{\Phi^c\}_c \rangle$

A transformation is described by a Completely-Positive-Trace-Preserving (CPTP) Map

$$\forall_c \, \Phi^c : \boldsymbol{H} \rightarrow \boldsymbol{H}$$

In the Kraus representation $\forall_c \, \Phi^c \Leftrightarrow \{K_i\}^c$

- $\Phi^c(\rho_x) = \sum_i K_i^c \rho_x K_i^{c\,\dagger}$

Complete Positivity: A map Φ is completely positive if, for any state ρ, $\Phi(\rho)$ is positive semi-definite. This ensures that no negative probabilities arise.

Trace Preservation: $Tr\big(\Phi(\rho)\big) = Tr(\rho)$ for all ρ.

To guarantee this property, the Kraus operators must satisfy : $\sum_i K_i^\dagger K_i = I$, where I is the identity operator on the Hilbert space $\boldsymbol{H}$.

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$\{\Phi^c\}_{c \in \{1,2\}}: \mathbb{C}^2 \rightarrow \mathbb{C}^2 \Leftrightarrow$

$$\Phi^1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \Phi^2 = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- $\Phi^1(\rho_x) = \rho_x$; $\Phi^2(\rho_x) = H \rho_x H^\dagger$

Special case, where transformations are given by unitaries U,i.e there is only one Kraus operator, the unitary itself, $U^\dagger U = I$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{\Phi^c\}_{c\,\in\{1,2\}}: \mathbb{C}^2 \rightarrow \mathbb{C}^2 \Leftrightarrow$

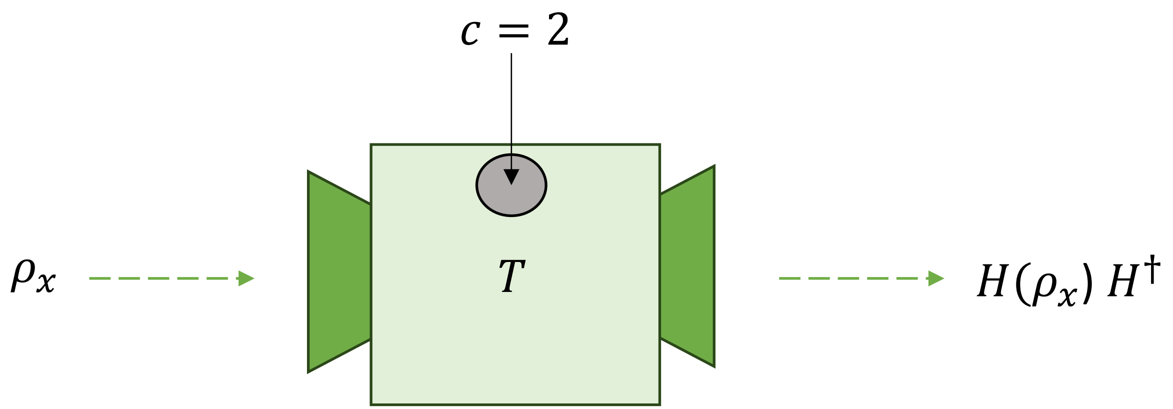
$$\Phi^1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \Phi^2 = H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- $\Phi^1(\rho_x) = \rho_x\ ;\ \Phi^2(\rho_x) = H\ \rho_x\ H^\dagger$

Special case, where transformations are given by unitaries U,i.e there is only one Kraus operator, the unitary itself, $U^\dagger\ U = I$

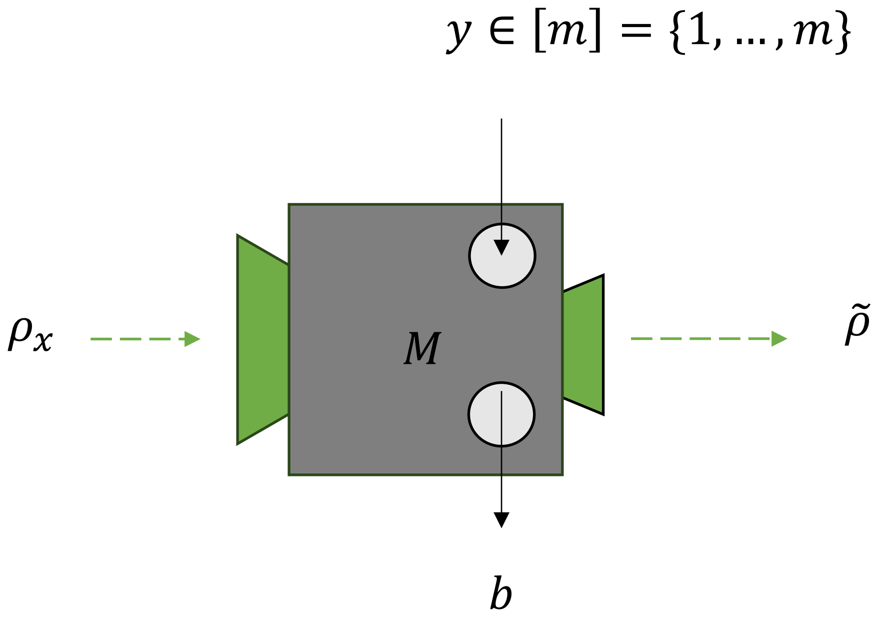
$\{|0\rangle, |1\rangle\}$ = Computational Basis

represented as $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix};\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

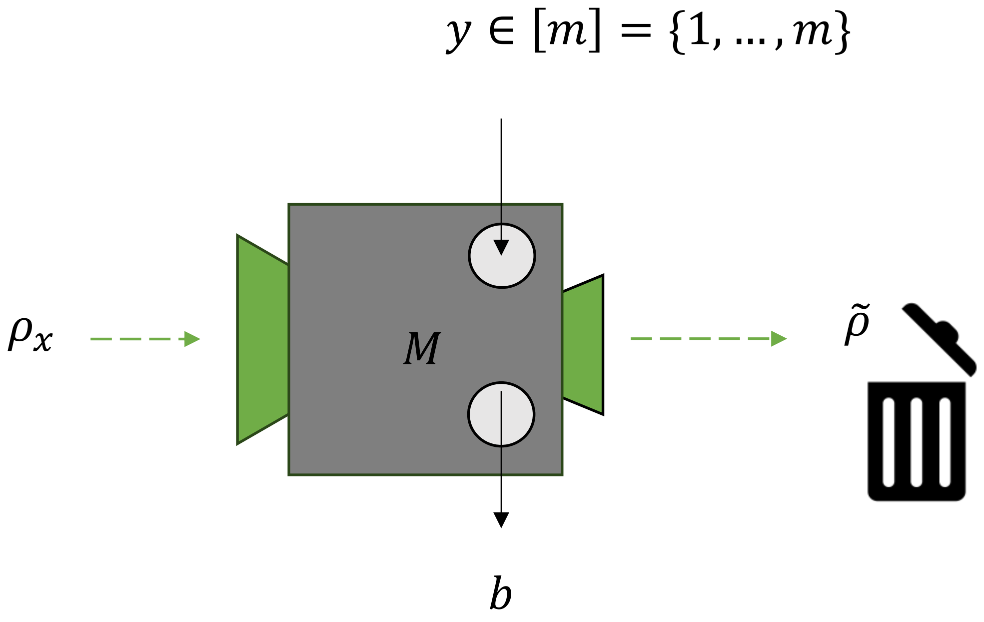


Measurements (non-destructive)

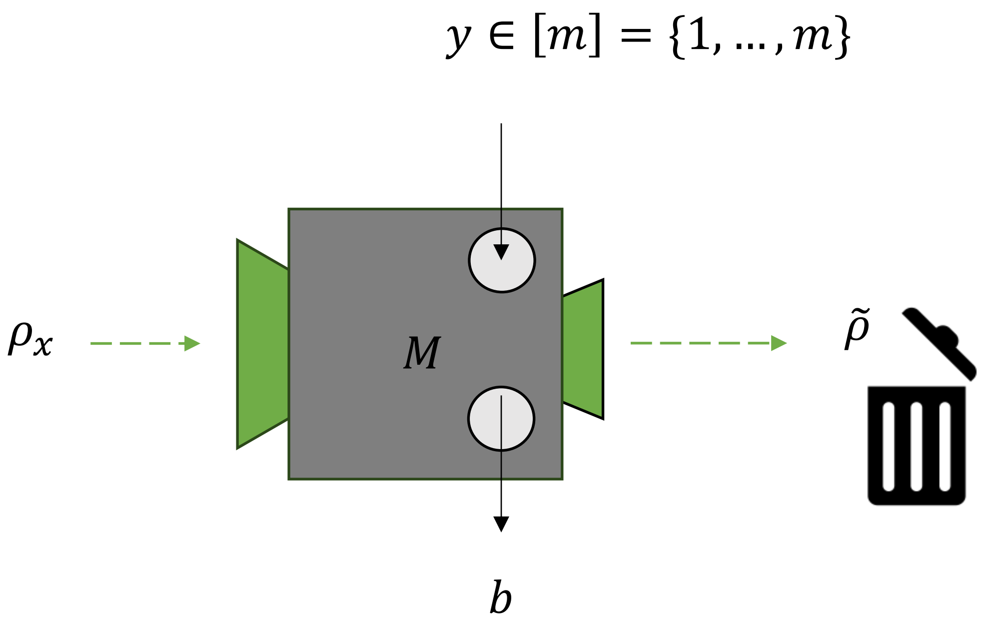
Measurements (non-destructive)



Measurements (non-destructive)

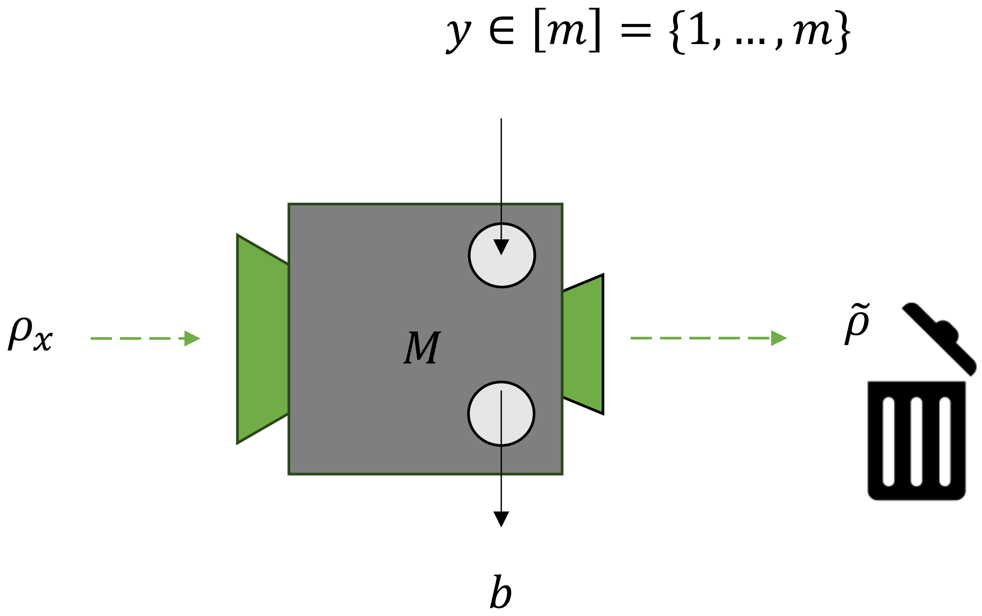


Measurements (non-destructive)



In the lab it might look more like this…

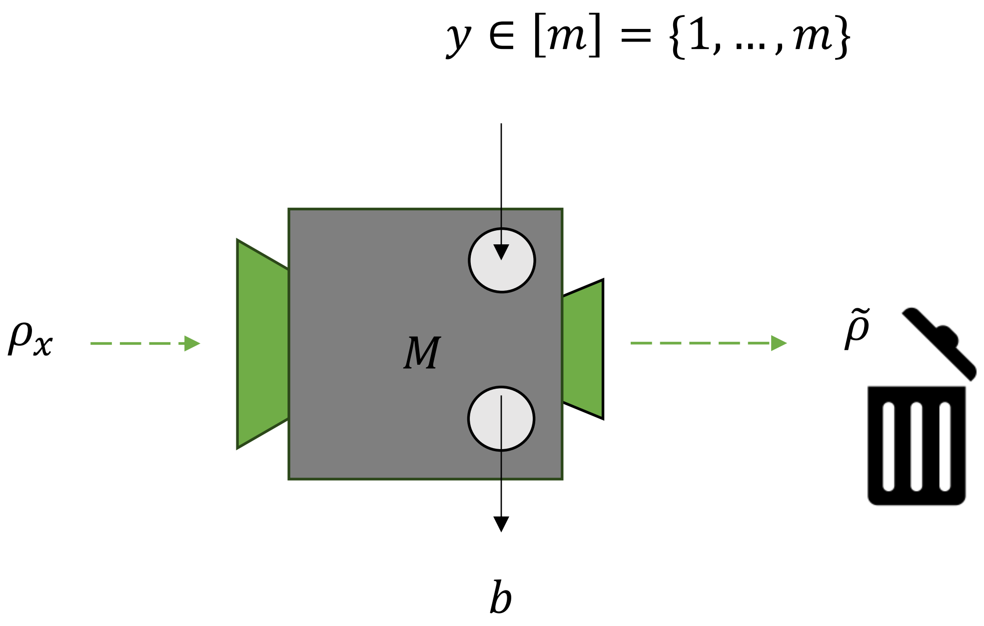
Measurements (non-destructive)



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Measurements (non-destructive)



In the lab it might look more like this…

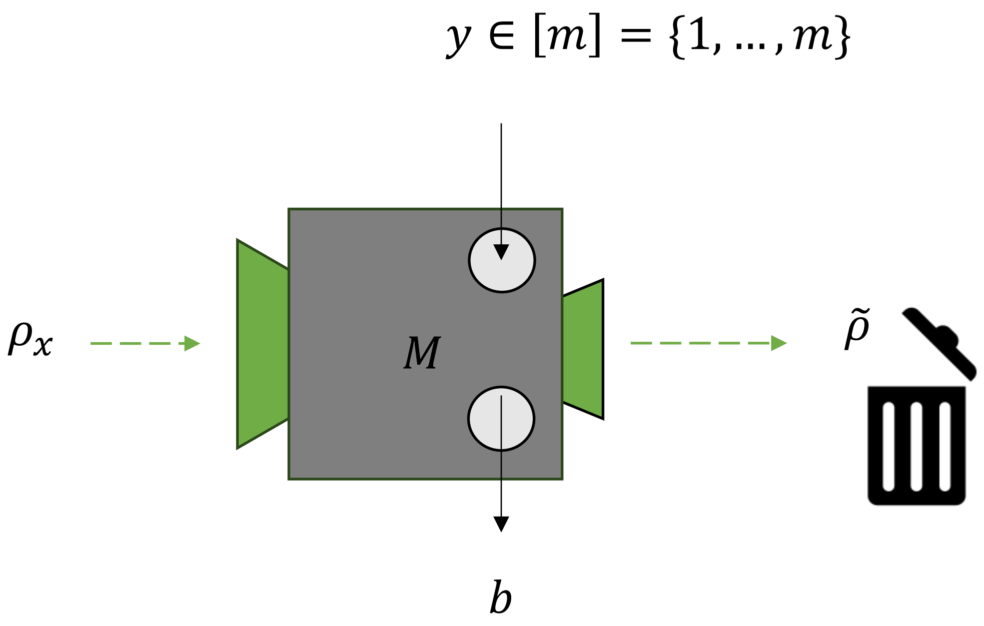
- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Hermiticity: $E_{b|y} = {E_{b|y}}^{\dagger}$

Positive Semi-Definiteness: For any vector $|\psi\rangle \in \boldsymbol{H}$, we have $\langle\psi | E_{b|y} | \psi\rangle \geq 0$. Equivalent to say that the spectrum, the set of eigenvalues, is non-negative.

Sum to identity: For all y, $\sum_b E_{b|y} = I_H$,

Measurements (non-destructive)



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.

Hermiticity: $E_{b|y} = E_{b|y}{}^{\dagger}$

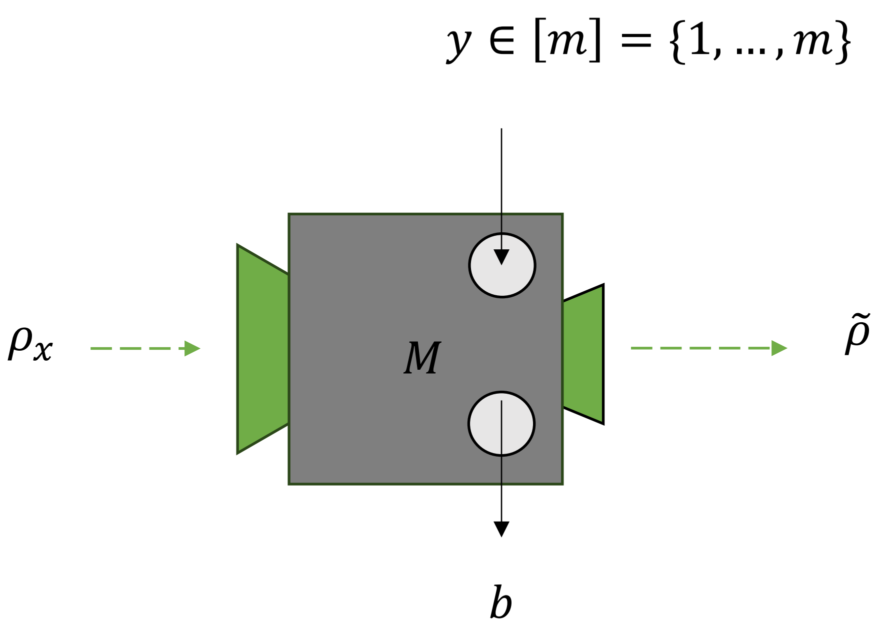
Positive Semi-Definiteness: For any vector $|\,\psi\rangle \in \boldsymbol{H}$, we have $\langle\psi\,|\,E_{b|y}\,|\,\psi\rangle \geq 0$. Equivalent to say that the spectrum, the set of eigenvalues, is non-negative.

Sum to identity: For all y, $\sum_b E_{b|y} = I_H$,

- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$p(b|y,x) = Tr(\rho_x\, E_{b|y})$$

Measurements (non-destructive)



In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.
- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$p(b|y,x) = Tr(\rho_x\, E_{b|y})$$

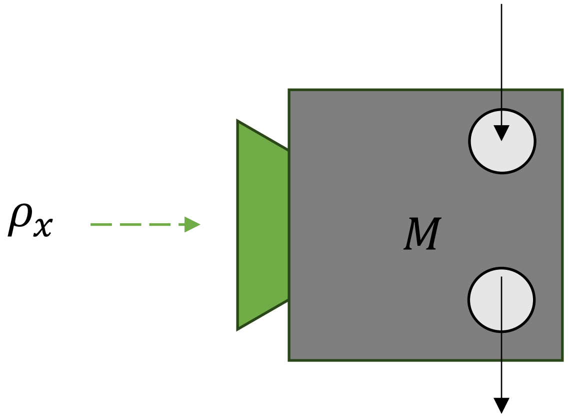
- For a non-destructive measurement the post-measurement state is

$$\rho_{\{x,y,b\}} = \frac{K_{b|y}\rho_x K_{b|y}{}^{\dagger}}{Tr(K_{b|y}\rho_x K_{b|y}{}^{\dagger})}$$

$$E_{b|y}{}^{\dagger} = K_{b|y}K_{b|y}{}^{\dagger}$$

Measurements (destructive)

$y \in [m] = \{1, \dots, m\}$



b

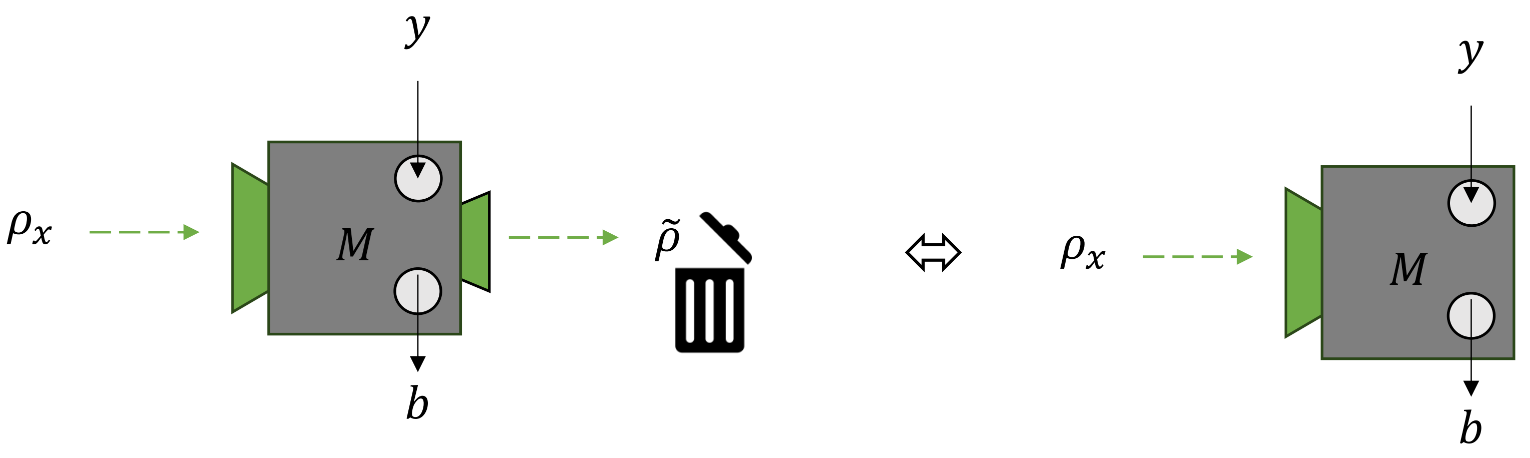
In the lab it might look more like this…

- $\langle \boldsymbol{H}, \{E_{b|y}\}_y \rangle$
  - $\{E_{b|y}\}$ is Positive Operator Valued Measure (POVMs)— a measurement is given by specifying one POVM for each choice of y. POVMs elements are positive semi-definite, Hermitian operators acting on a Hilbert space $\boldsymbol{H}$.
- Probability of outcome b for POVM defined by y, and state prepared by x is given by the Born rule as follows,

$$p(b|y,x) = Tr(\rho_x \, E_{b|y})$$

- For a destructive measurement there is no post-measurement state

Operationally, to trash the system is equivalent to assume that it did not exist.



First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{E_{b|y}\} \Leftrightarrow \quad \{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\},$

$\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\},$

Special case, where the POVM elements are projections, $P^2 = P$.

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

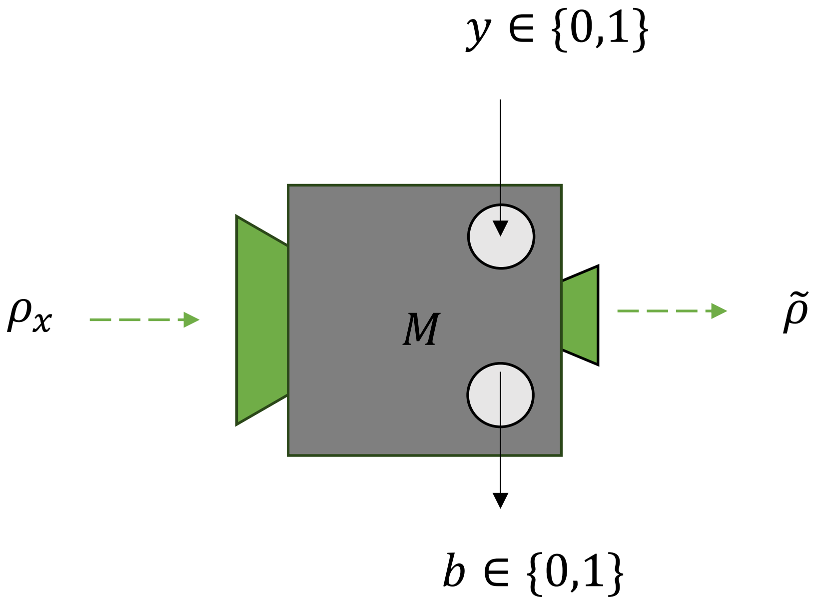
$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$$\{E_{b|y}\} \Leftrightarrow \quad \{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\},$$

$$\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\},$$

Special case, where the POVM elements are projections, $P^2 = P$.



$$p(0|0, x) = Tr(\rho_x |0\rangle\langle 0|) \Rightarrow \tilde{\rho} = |0\rangle\langle 0|$$

$$p(1|0, x) = Tr(\rho_x |1\rangle\langle 1|) \Rightarrow \tilde{\rho} = |1\rangle\langle 1|$$

$$p(0|1, x) = Tr(\rho_x |+\rangle\langle +|) \Rightarrow \tilde{\rho} = |+\rangle\langle +|$$

$$p(1|1, x) = Tr(\rho_x |-\rangle\langle -|) \Rightarrow \tilde{\rho} = |-\rangle\langle -|$$

First, define the space:

- $\boldsymbol{H} = \mathbb{C}^2$

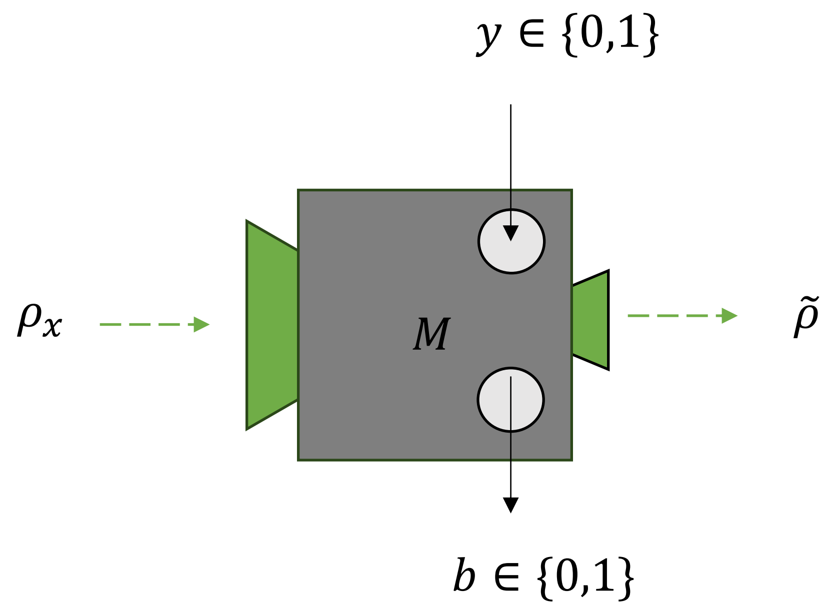
$Span\{|0\rangle, |1\rangle\}$

2D Quantum system = Qubit

$\{E_{b|y}\} \Leftrightarrow \quad \{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\},$

$\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\},$

Special case, where the POVM elements are projections, $P^2 = P$.



$p(0|0,x) = Tr(\rho_x|0\rangle\langle 0|) \Rightarrow \tilde{\rho} = |0\rangle\langle 0|$

$p(1|0,x) = Tr(\rho_x|1\rangle\langle 1|) \Rightarrow \tilde{\rho} = |1\rangle\langle 1|$

$p(0|1,x) = Tr(\rho_x|+\rangle\langle +|) \Rightarrow \tilde{\rho} = |+\rangle\langle +|$

$p(1|1,x) = Tr(\rho_x|-\rangle\langle -|) \Rightarrow \tilde{\rho} = |-\rangle\langle -|$

Calculating the post-measurement state for projective measurements is easier, it is just the state associated with the classical value registered y.

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T; \; P < M;$

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T$; $P < M$;
- $T < T$; $T < M$;

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T$; $P < M$;
- $T < T$; $T < M$;
- $(M < M)$; $(M < T)$;

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T;\ P < M;$
- $T < T;\ T < M;$
- $(M < M); (M < T);$

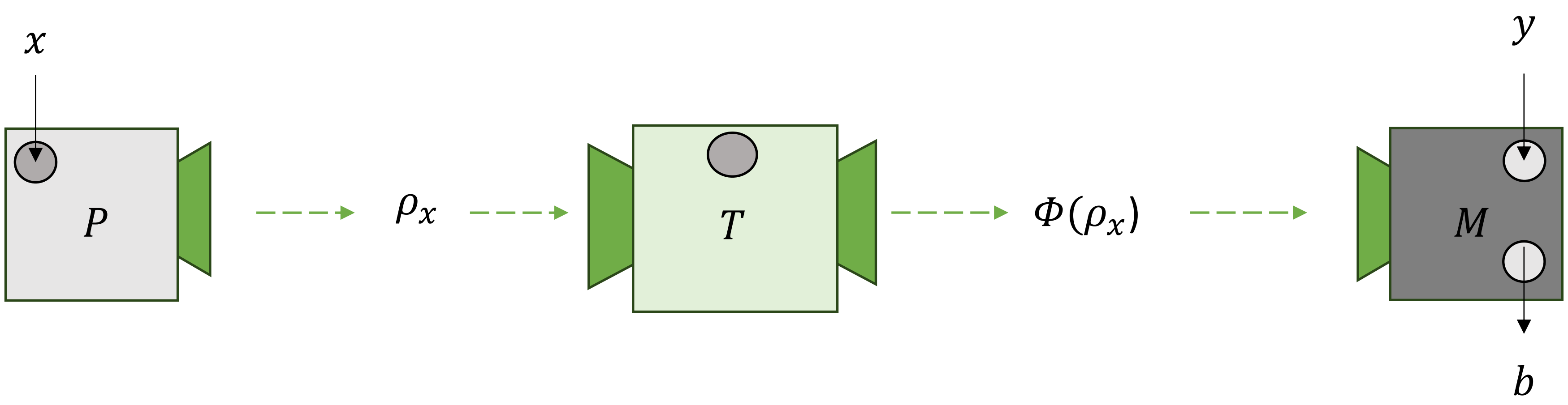
What is the simplest diagram using: 1 Preparation, 1 Transformation and 1 Measurement?

Now that we have the boxes defined…

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T;\ P < M;$
- $T < T;\ T < M;$
- $(M < M);(M < T);$

What is the simplest diagram using: 1 Preparation, 1 Transformation and 1 Measurement?

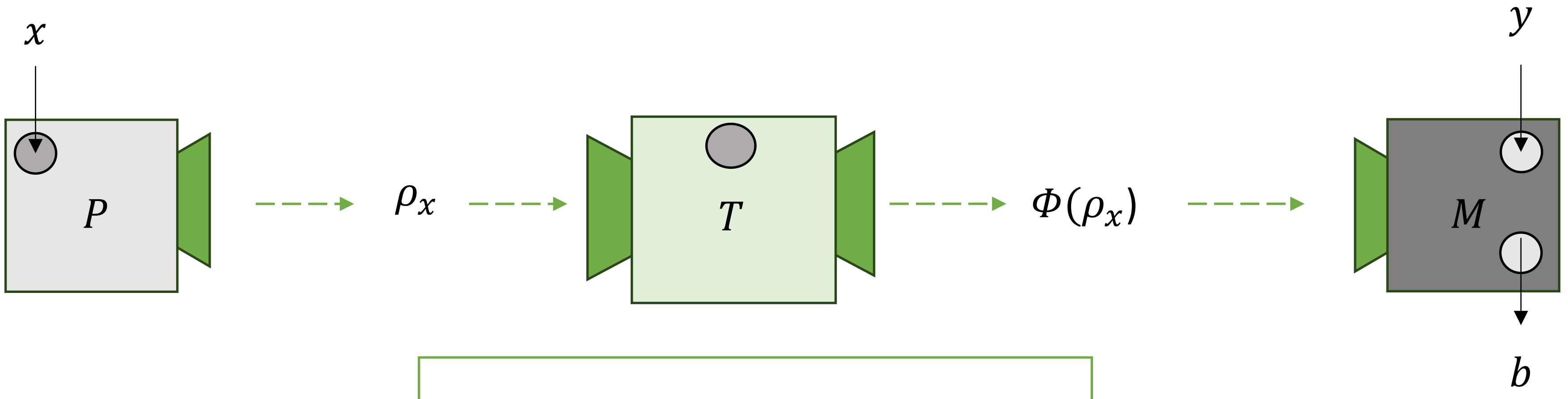


Now that we have the boxes defined…

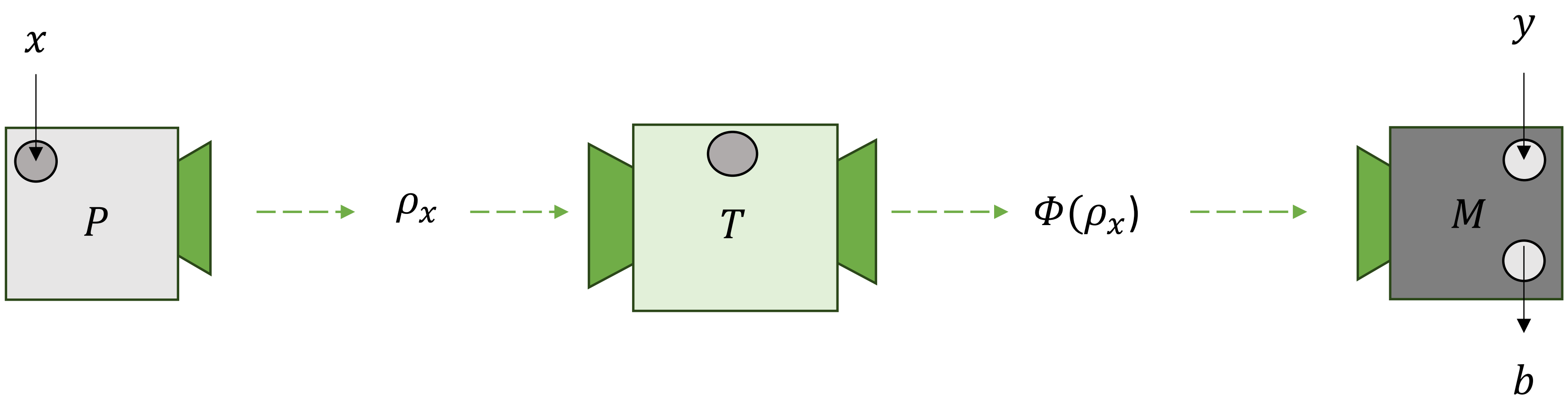
How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:
Quantum outputs can connect to quantum inputs

- $P < T;\ P < M;$
- $T < T;\ T < M;$
- $(M < M); (M < T);$

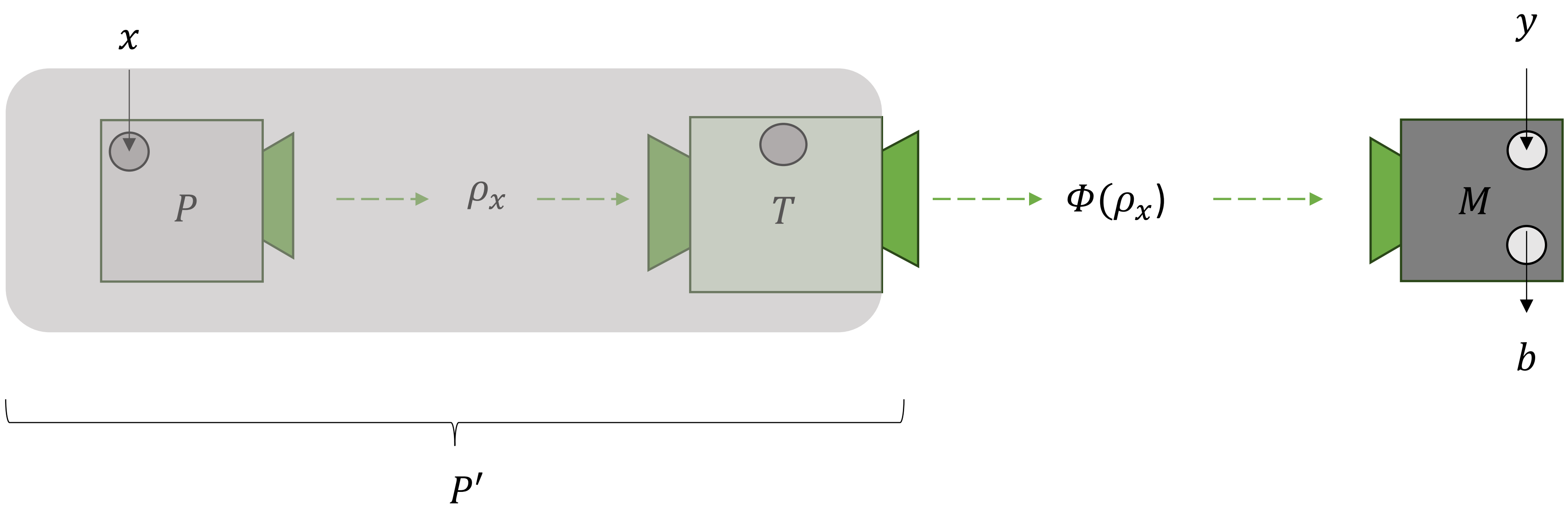
What is the simplest diagram using: 1 Preparation, 1 Transformation and 1 Measurement?

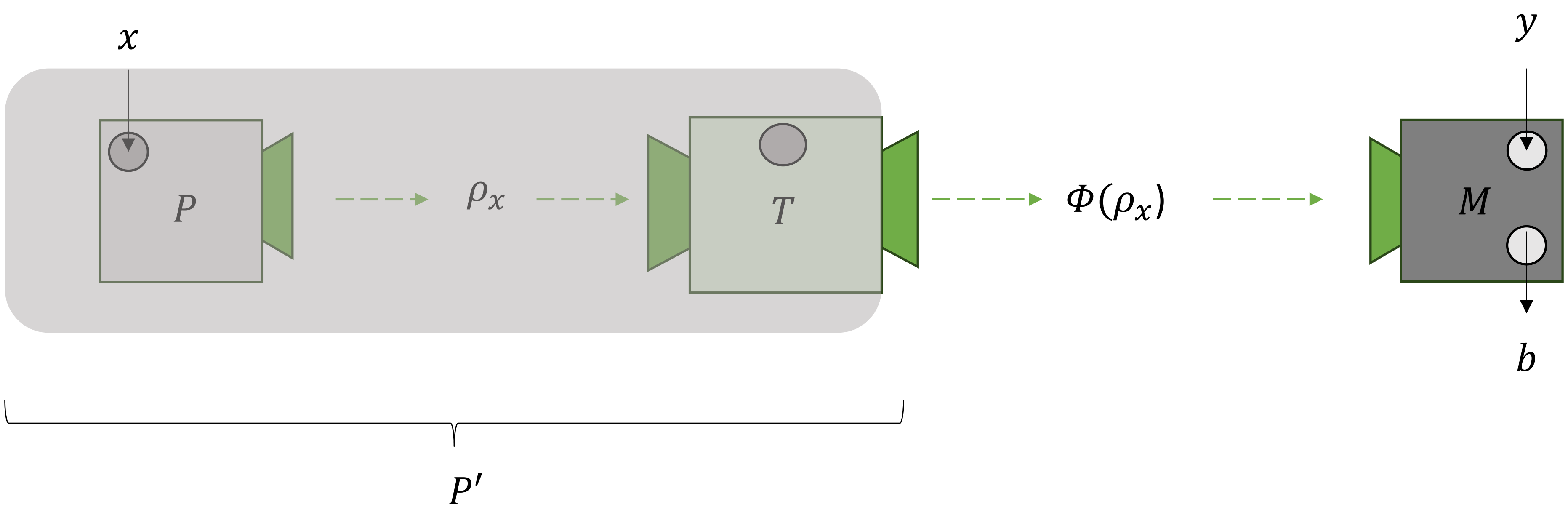


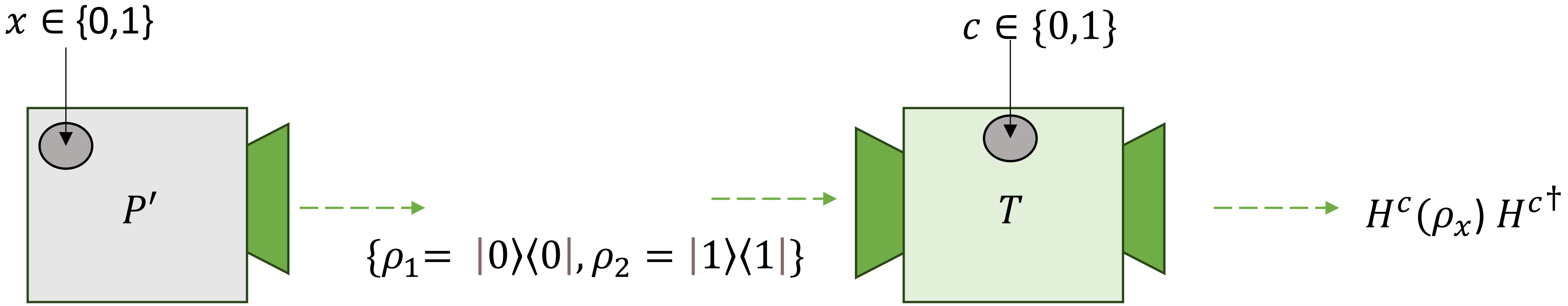
$$p(b|y,x) = Tr(\Phi(\rho_x)E_{b|y})$$



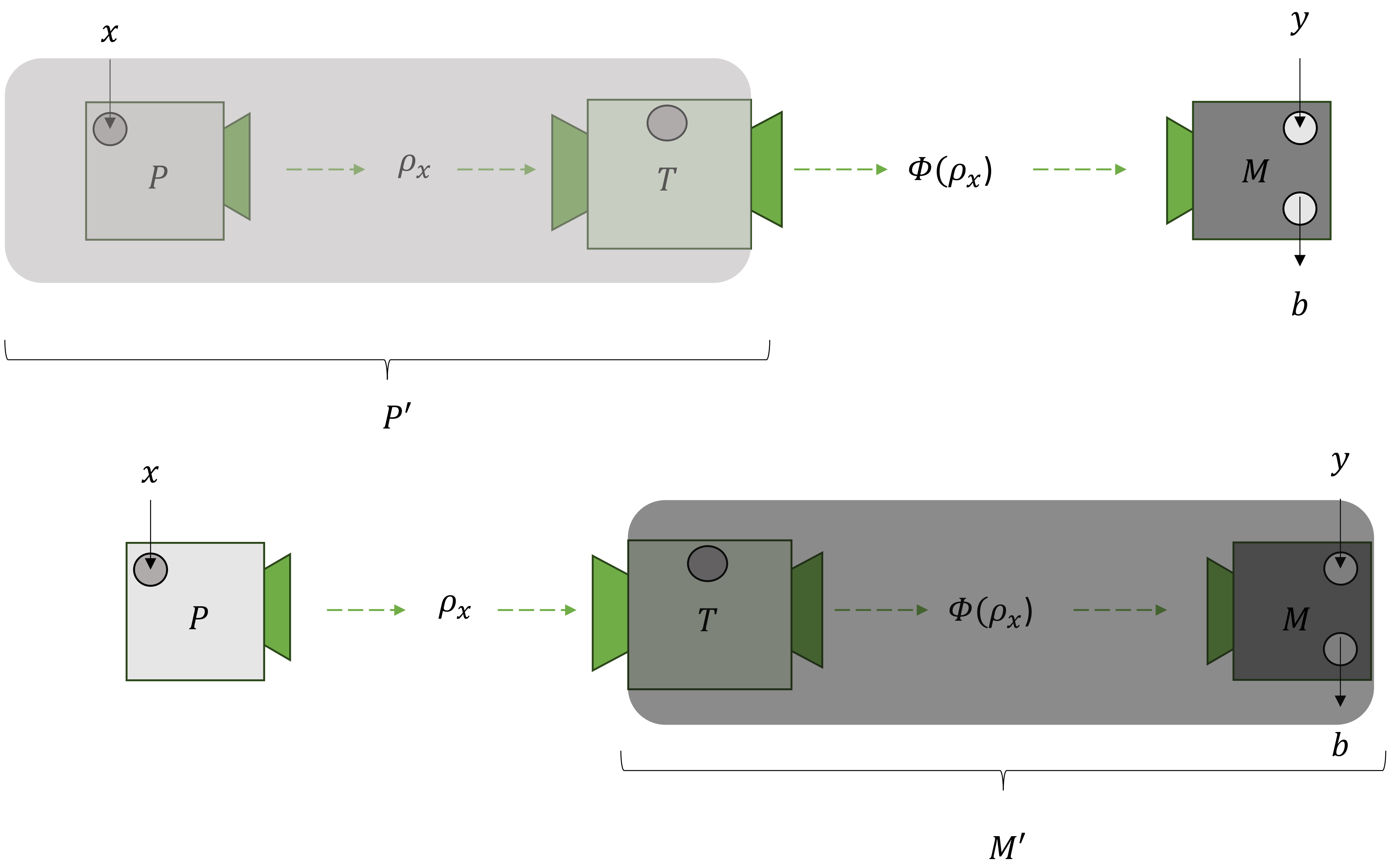
x
P
ρ_x
T
$\Phi(\rho_x)$
y
M
b


x
P
ρ_x
T
Φ(ρ_x)
M
y
b
P′





This is equivalent to the original example of the preparation we saw.


x
P
ρ_x
T
Φ(ρ_x)
y
M
b
P′
x
P
ρ_x
T
Φ(ρ_x)
y
M
b
M′

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:

Quantum outputs can connect to quantum inputs (ignoring Transformations)

- $P < M; \;\; (M < M);$

How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:

Quantum outputs can connect to quantum inputs (ignoring Transformations)

- $P < M; \;\; (M < M);$

We are going to focus only on Preparation and Measurements.
What is the simplest diagram using: 1 Preparation and 1 Measurement? There is only one…

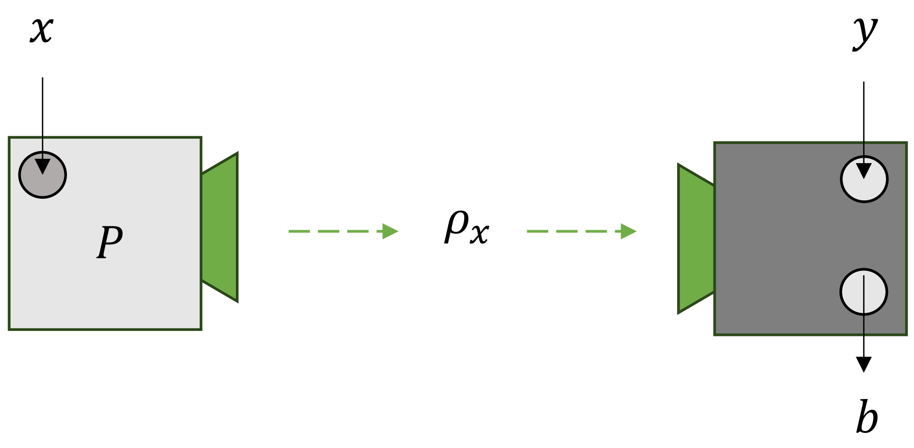
How to connect the boxes? Compositional rules for connecting the quantum systems using black-boxes:

Quantum outputs can connect to quantum inputs (ignoring Transformations)

- $P < M; \ \ (M < M);$

We are going to focus only on Preparation and Measurements.
What is the simplest diagram using: 1 Preparation and 1 Measurement? There is only one…

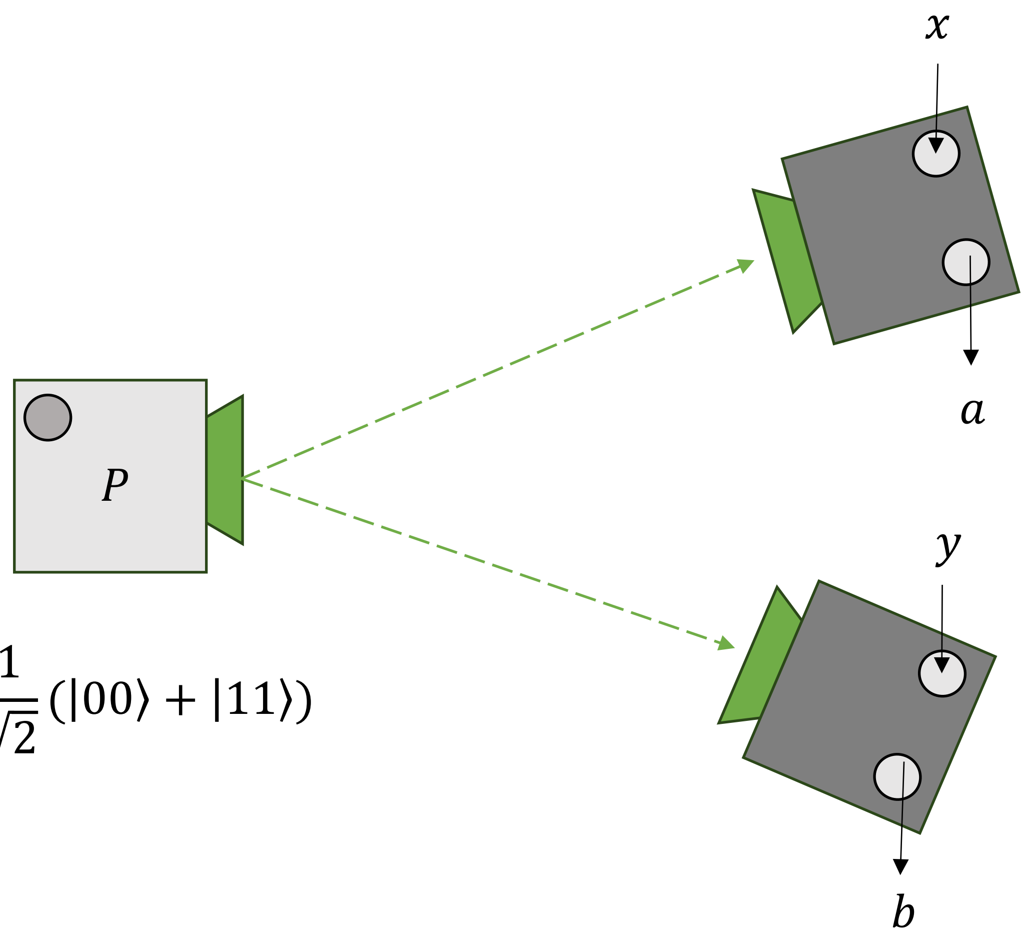
Prepare and Measure scenario



$$p(b|y,x) = Tr(\rho_x E_{b|y})$$

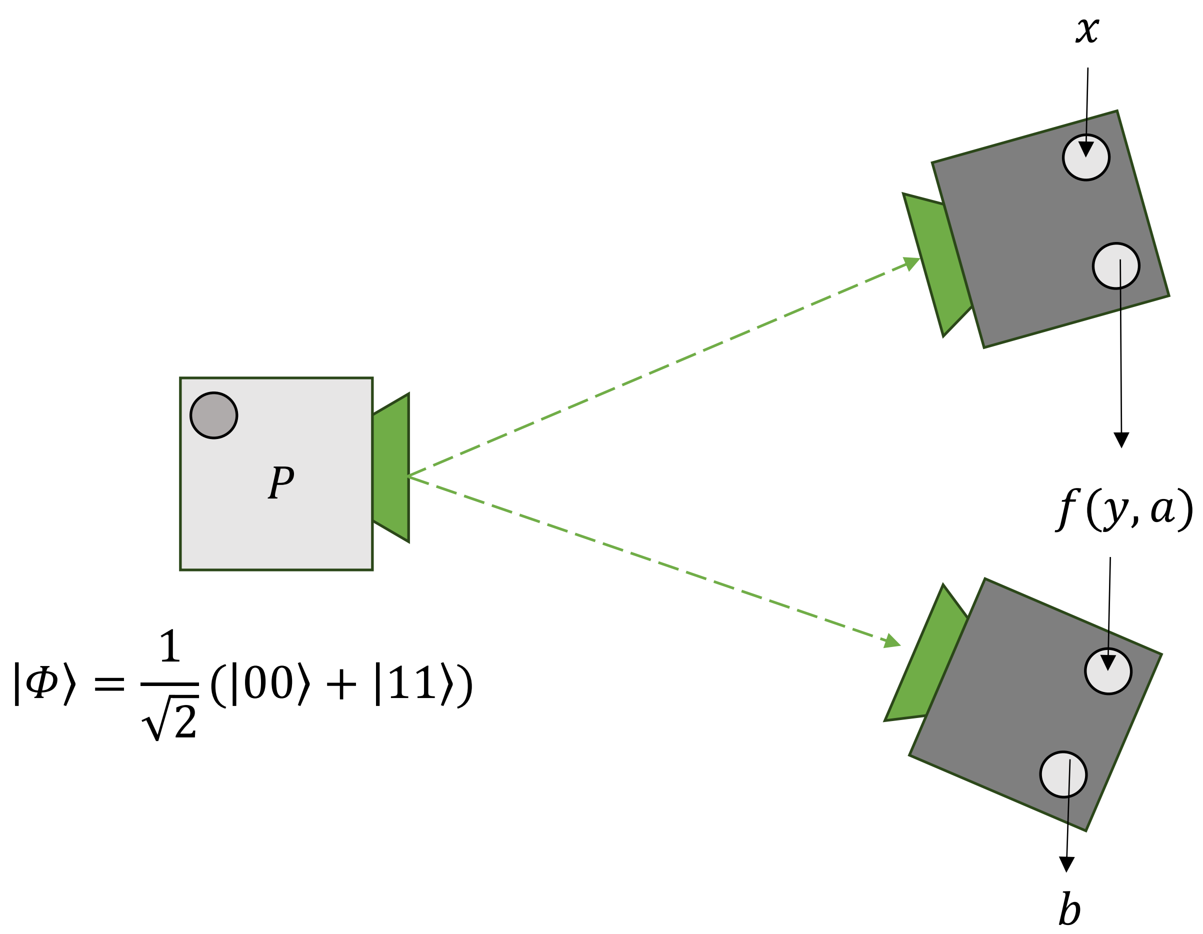
1 Preparation and 2 Measurements ?

1 Preparation and 2 Measurements: Bi-partite Bell (Nonlocality)

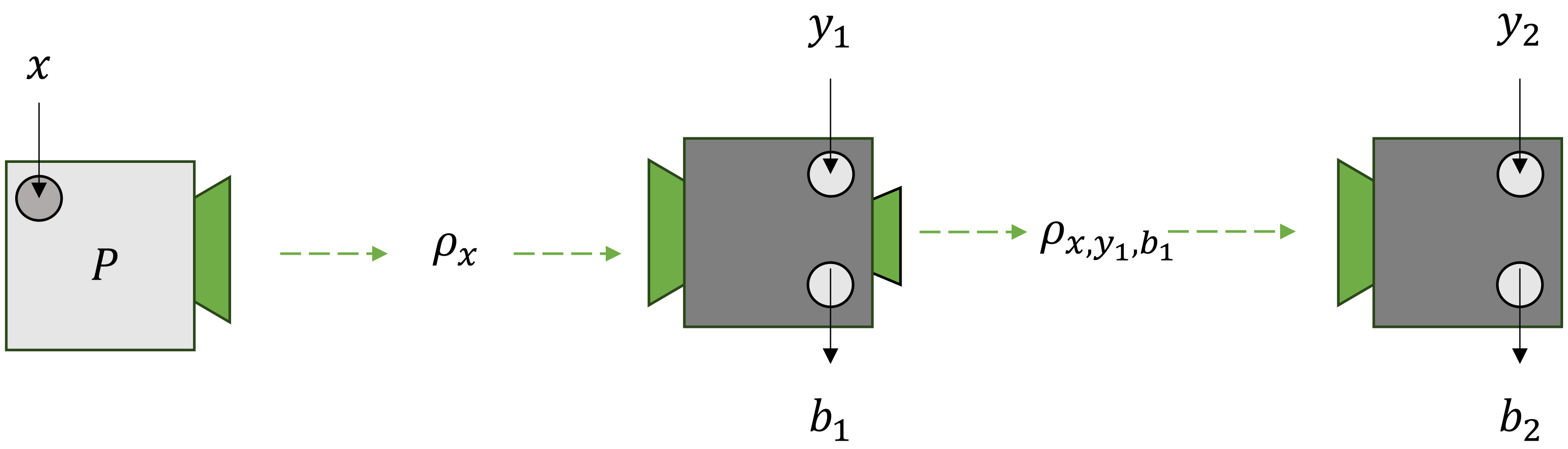


$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

1 Preparation and 2 Measurements: Bi-partite Bell w/ restricted classical communication



1 Preparation and 2 Measurements: Sequential Measurement Scenario with two measurements (Legget-Garg Inequalities, Temporal correlation, KS-Contextuality)



1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

- Bi-local scenario
- Entanglement-assisted PM

1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

- Bi-local scenario
- Entanglement-assisted PM

… and many more!

1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

- Bi-local scenario
- Entanglement-assisted PM

… and many more!

Reduced to a caricature, the operational perspective could be read to say

1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

- Bi-local scenario
- Entanglement-assisted PM

… and many more!

Reduced to a caricature, the operational perspective could be read to say

- Quantum Information = Finding interesting ways to connect boxes;

1 Preparation and 3 Measurements:

- Tripartite Bell
- Bi-partite hidden nonlocal scenario (1 measurement for A and 2 for Bob)
- Sequential Scenario with 3 Measurements

2 Preparations and (up to) 4 Measurements:

- Bi-local scenario
- Entanglement-assisted PM

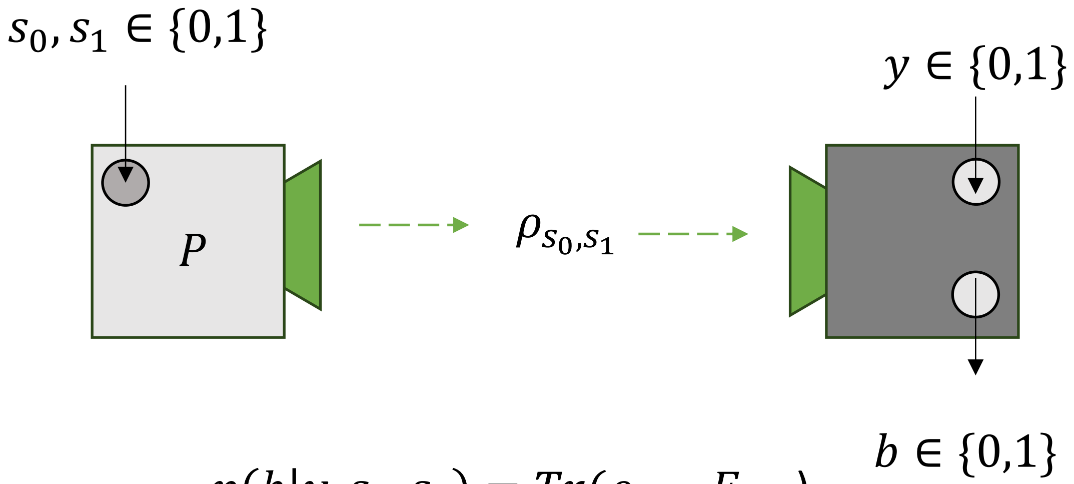
… and many more!

Reduced to a caricature, the operational perspective could be read to say

- Quantum Information = Finding interesting ways to connect boxes;
- Quantum Cryptography = Finding interesting ways to <u>securely</u> connect boxes;

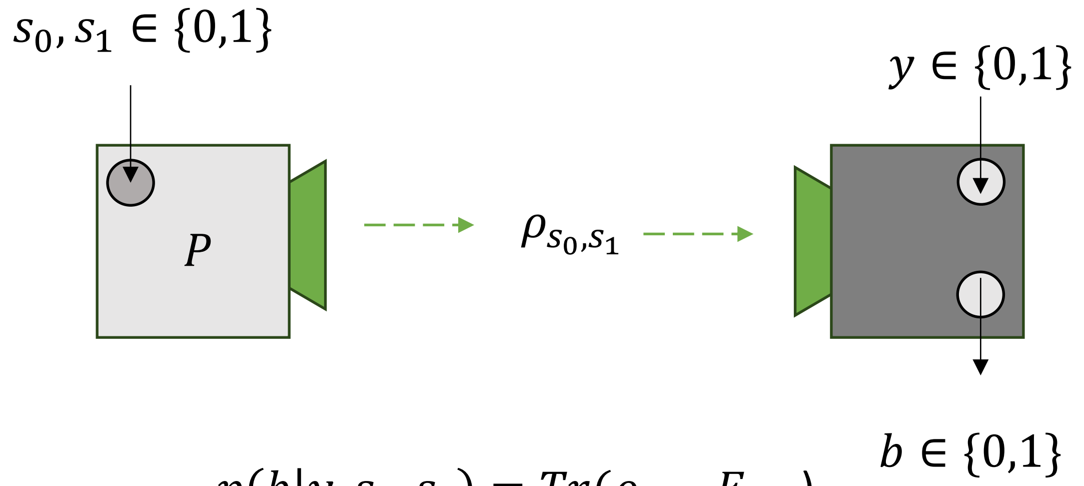
Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.

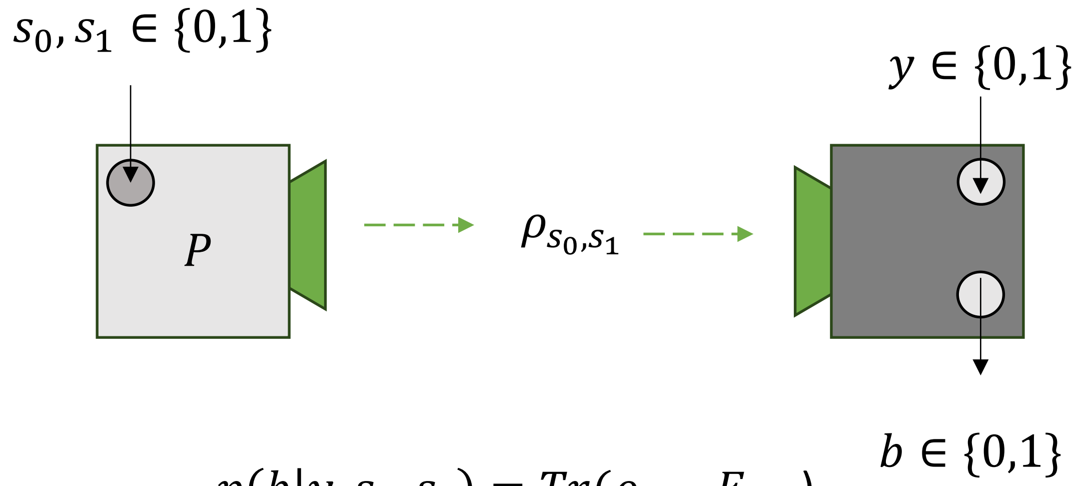


$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

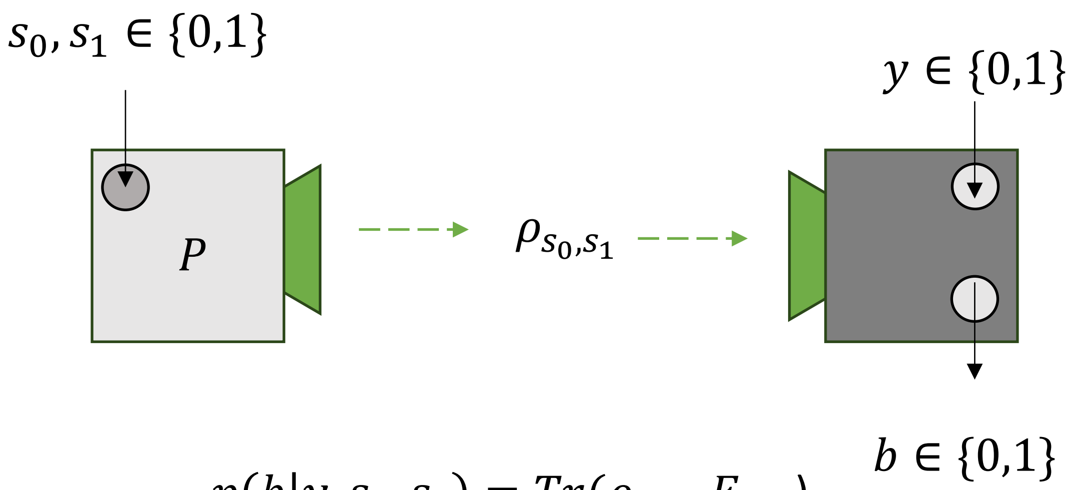
Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

Define the measurements:

- $\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\}$
- $\{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\}$,

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

Define the measurements:

- $\{E_{0|1} = |+\rangle\langle +| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, E_{1|1} = |-\rangle\langle -| = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}\}$
- $\{E_{0|0} = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{1|0} = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\}$,

$p(b = s_0|y = 0, s_0, s_1 = 0) = 1$

$p(b \neq s_0|y = 0, s_0, s_1 = 0) = 0$

$p(b = s_0|y = 1, s_0, s_1 = 0) = 1/2$

$p(b \neq s_0|y = 1, s_0, s_1 = 0) = 1/2$

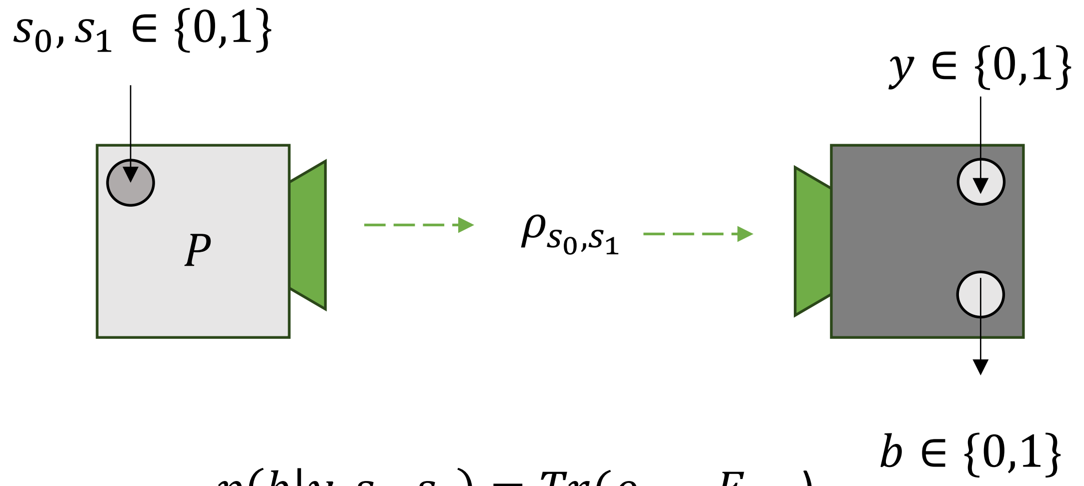
$p(b = s_0|y = 1, s_0, s_1 = 1) = 1$

$p(b \neq s_0|y = 1, s_0, s_1 = 1) = 0$

$p(b = s_0|y = 0, s_0, s_1 = 1) = 1/2$

$p(b \neq s_0|y = 0, s_0, s_1 = 1) = 1/2$

Going back to the Prepare and Measure scenario,
which although the simplest is of fundamental importance to quantum crypto.



$$p(b|y, s_0, s_1) = Tr(\rho_{s_0,s_1} E_{b|y})$$

Define the density operators for the possible inputs:

- $\{\rho_{00} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \rho_{01} = |+\rangle\langle +|, \rho_{11} = |-\rangle\langle -|\}$

These states form Mutually Unbiased Basis (or Conjugate Basis) i.e. Computational and Diagonal, these are states such that, when projected to the other basis no information is obtained about the state of the system.

This is the basic idea of Wiesner's Conjugate Coding paper:

A conjugate code is any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems. Note that in the

This is the basic idea of Wiesner's Conjugate Coding paper:

> A conjugate code is any communication scheme in which the physical systems used as signals are placed in states corres-ponding to elements of several conjugate basis of the Hilbert space describing the individual systems. Note that in the

Thes scheme is the building block for:

- The first Quantum Oblivious Transfer (QOT) protocol proposed;
- The Bennet-Brassard QKD protocol (BB84)

… and even some recent work from IT-Aveiro (Q-OLE by M. Santos et al)

This is the basic idea of Wiesner's Conjugate Coding paper:

A conjugate code is any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems. Note that in the

Thes scheme is the building block for:

- The first Quantum Oblivious Transfer (QOT) protocol proposed;
- The Bennet-Brassard QKD protocol (BB84)

… and even some recent work from IT-Aveiro (Q-OLE by M. Santos et al)

But even in the original conjugate coding, Wiesner already gave two applications of this idea. As we will see, under some very strong assumptions, the first example can already be rightfully claimed to be an OT.

First application of Conjugate Coding:

Example One: A means for transmitting two messages either but not both of which may be received.

First application of Conjugate Coding:

Example One: A means for transmitting two messages either but not both of which may be received.

$string_1 = 0010100 \ldots$ $q.encoding_1 = |0\rangle\langle 0|, |0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 0| \ldots$

$string_2 = 1011100 \ldots$ $q.econding_2 = |-\rangle\langle -|, |+\rangle\langle +|, |-\rangle\langle -| \ldots$

First application of Conjugate Coding:

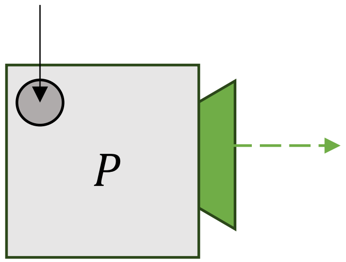
Example One: A means for transmitting two messages either but not both of which may be received.

$string_1 = 0010100 \ldots$ $\quad$ $q.encoding_1 = |0\rangle\langle 0|, |0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 0| \ldots$

$string_2 = 1011100 \ldots$ $\quad$ $q.econding_2 = |-\rangle\langle -|, |+\rangle\langle +|, |-\rangle\langle -| \ldots$

$For\ i\ rounds, r_i \underset{\$}{\leftarrow} \{1,2\}$:

$string_{r_i}[i]$



$q.encoding_{r_i}[i]$

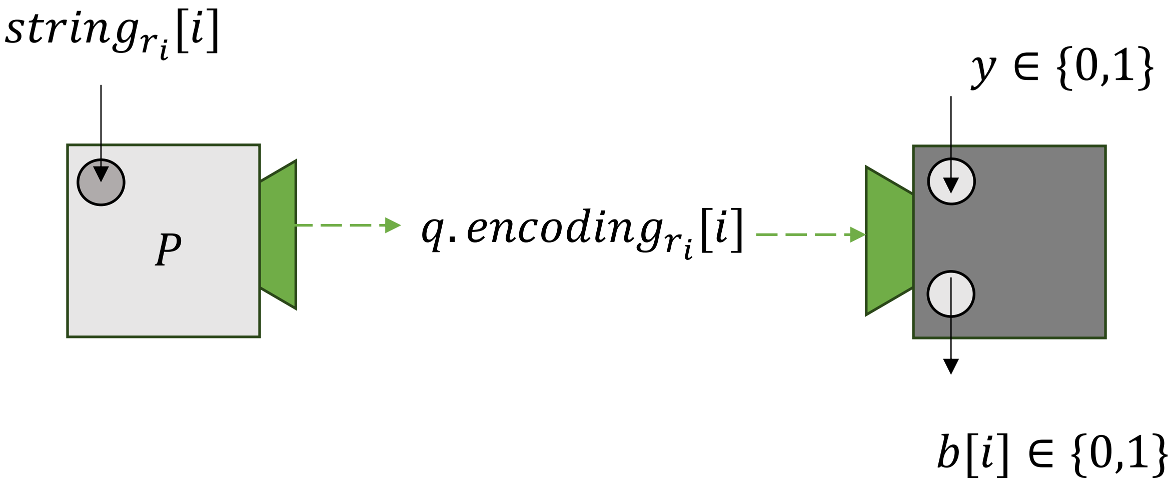
First application of Conjugate Coding:

Example One: A means for transmitting two messages either but not both of which may be received.

$string_1 = 0010100 \ldots$ $\quad q.encoding_1 = |0\rangle\langle 0|, |0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 0| \ldots$

$string_2 = 1011100 \ldots$ $\quad q.econding_2 = |-\rangle\langle -|, |+\rangle\langle +|, |-\rangle\langle -| \ldots$

$For\ i\ rounds, r_i \underset{\$}{\leftarrow} \{1,2\}$:



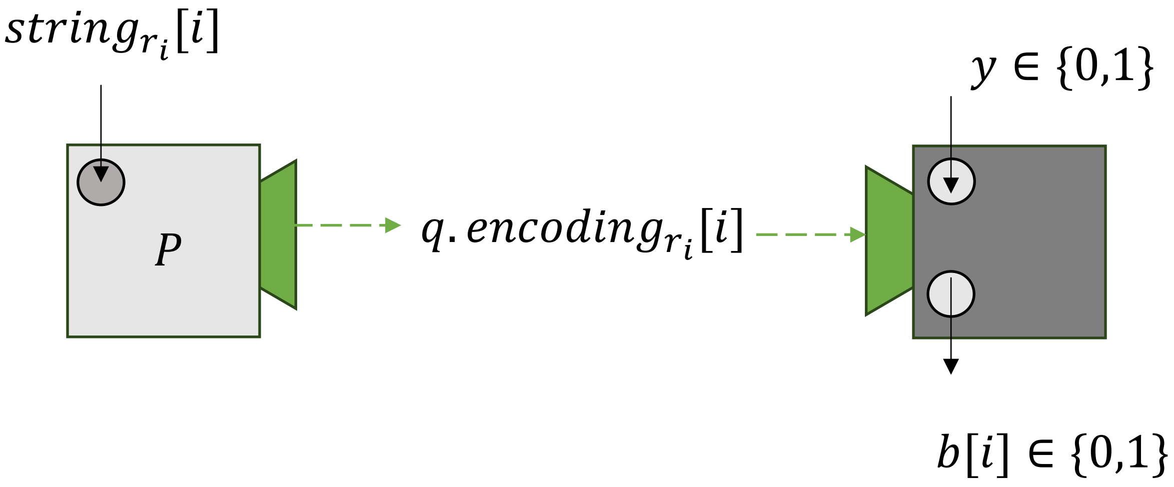
First application of Conjugate Coding:

Example One: A means for transmitting two messages either but not both of which may be received.

$string_1 = 0010100\ldots$ $\quad q.encoding_1 = |0\rangle\langle 0|, |0\rangle\langle 0|, |1\rangle\langle 1|, |0\rangle\langle 0| \ldots$

$string_2 = 1011100\ldots$ $\quad q.econding_2 = |-\rangle\langle -|, |+\rangle\langle +|, |-\rangle\langle -| \ldots$

$For\ i\ rounds, r_i \xleftarrow[\$]{} \{1,2\}$:



Bob’s measurement is not so good, so it needs to fix à priori the y globally for all rounds.

So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won’t know what was the message that Bob recovered since there is no information going from Bob to Alice.

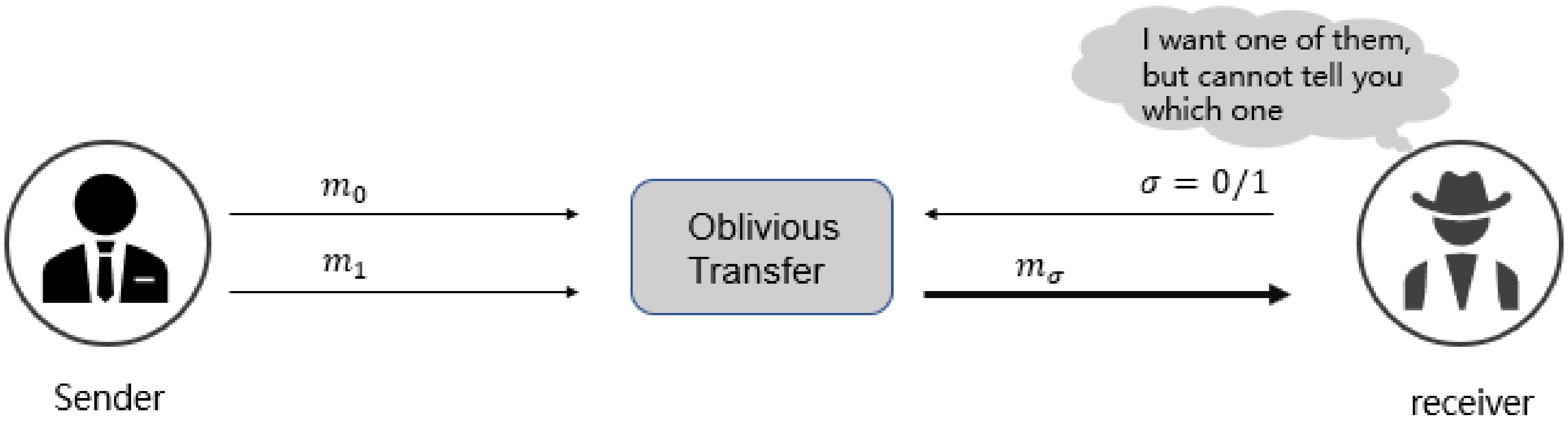
So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

⇓

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.

So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.



So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.

- It is perfectly secure against a malicious Sender/Alice;
- It is secure against a semi-honest Receiver/Bob, for a trusted model of non-adaptative single qubit measurements

So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

⇩

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.

- It is perfectly secure against a malicious Sender/Alice;
- It is secure against a semi-honest Receiver/Bob, for a trusted model of non-adaptative single qubit measurements

Collective measurements are a problem.
Solved with extra physical assumptions on the trusted model, or computational assumptions.

So in the end, Bob can either recover a noisy string 1 or a noisy string 2, according to his choice, but not both.
Furthermore, Alice won't know what was the message that Bob recovered since there is no information going from Bob to Alice.

⇓

This is a 1-out-of-2 OT ! Introduced much before Rabin's 1981 proposal.

- It is perfectly secure against a malicious Sender/Alice;
- It is secure against a semi-honest Receiver/Bob, for a trusted model of non-adaptative single qubit measurements

Collective measurements are a problem.
Solved with extra physical assumptions on the trusted model, or computational assumptions.

For the next time!

Thanks!

(You can ask me for references, I forgot to put them on the slides)