Randomness and laws of nature: the QBist perspective

Rüdiger Schack
Royal Holloway, University of London

STIAS, October 2015

Problem solved?

Kelly Richdale kelly.richdale@idquantique.com via b2b 13 Oct (12 days ago) ☆

to Ruediger

QUANTIS TRUE RANDOM NUMBER GENERATOR

True Random Number Generation from the market leaders in reliability and certification. Swiss quantum engineering you can trust.

PRICE DROP

Quantis USB 4M Module

Now available for just €990

- 4Mbps of true quantum randomness
- Certified by Swiss National Laboratory

ORDER ONLINE NOW

Unseeded quantum random number generator (QRNG)

- A box.
- No input.
- Output: a bit string.
- The physical properties of the box guarantee that the output has a uniform distribution.

Key observation

An unseeded QRNG is not certifiable.

Plan for the talk

- Certifying randomness
- Locality and hidden variables
- Interpreting probability
- QBism
- Autonomy versus intrinsic randomness

“Certified by Swiss National Laboratory”

How does one certify an unseeded QRNG?

“Certified by Swiss National Laboratory”

How does one certify an unseeded QRNG?

Certify using randomness tests?

Problem: Tests cannot distinguish the output of a QRNG from that of a cryptographically strong PRNG.

“Certified by Swiss National Laboratory”

How does one certify an unseeded QRNG?

Certify using randomness tests?

Problem: Tests cannot distinguish the output of a QRNG from that of a cryptographically strong PRNG.

Certify by checking physical components?

Problem 1: You need to trust quantum physicists.

“Certified by Swiss National Laboratory”

How does one certify an unseeded QRNG?

Certify using randomness tests?

Problem: Tests cannot distinguish the output of a QRNG from that of a cryptographically strong PRNG.

Certify by checking physical components?

Problem 1: You need to trust quantum physicists.
Problem 2: What if an adversary tampers with the device?

“Certified by Swiss National Laboratory”

How does one certify an unseeded QRNG?

Certify using randomness tests?

Problem: Tests cannot distinguish the output of a QRNG from that of a cryptographically strong PRNG.

Certify by checking physical components?

Problem 1: You need to trust quantum physicists.
Problem 2: What if an adversary tampers with the device?
Problem 3: The nature of the quantum formalism (this talk).

Device independent (DI) QRNG

(Very) incomplete history:

Device independent (DI) QRNG

(Very) incomplete history:

- Braunstein and Caves (chained Bell inequalities)
- Kent and Barrett (DI QKD)
- Colbeck (the idea for a DI QRNG)
- Pironio et al. (construction of a DI QRNG)
- Colbeck and Renner (no need for perfect input bits)

Device independent (DI) QRNG

- Two boxes, A and B.

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.
- They generate output strings x and y.

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.
- They generate output strings x and y.
- a and b are random.

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.
- They generate output strings x and y.
- a and b are random.
- There is no signaling between the boxes (i.e., $P(x|a,b) = P(x|a)$ and vice versa).

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.
- They generate output strings x and y.
- a and b are random.
- There is no signaling between the boxes (i.e., $P(x|a,b) = P(x|a)$ and vice versa).
- The strings a, b, x, y violate certain inequalities.

Device independent (DI) QRNG

- Two boxes, A and B.
- They receive input strings a and b.
- They generate output strings x and y.
- a and b are random.
- There is no signaling between the boxes (i.e., $P(x|a,b) = P(x|a)$ and vice versa).
- The strings a, b, x, y violate certain inequalities.
- Then x and y are ("certifiably") random.

DI QRNG versus PRNG

A DI QRNG is unlike a PRNG:

1. it does not depend on computational assumptions;
2. it can generate uniform randomness from a partially random seed.

DI QRNG versus PRNG

A DI QRNG is unlike a PRNG:

1. it does not depend on computational assumptions;
2. it can generate uniform randomness from a partially random seed.

A DI QRNG is like a PRNG:

both depend on the randomness of an input seed.

DI QRNG: Prerequisites

- A random seed.
- No signaling between the boxes.
- Data that violate Bell inequalities.
- And it's useful only because one cannot certify an unseeded QRNG

Locality

- Locality is the idea that "an object is directly influenced only by its immediate surroundings".
- Einstein didn't "see how physical laws could be formulated and tested without [it]."
- And yet there are claims everywhere that nature is nonlocal (e.g., NYT October 21, 2015).

What is going on?

Ontological models (a.k.a. hidden variable models)

For any measurement, the outcome probabilities are determined by the system's real properties. (Harrigan and Spekkens, 2007).

Assuming hidden variables is closely related to a mechanistic world view ("the world is a randomized algorithm").

Loophole-free Bell experiment

You have to give up either locality or hidden variables.

Assuming you don't want to give up both, your choices are:

Nonlocal hidden variables

(1) Probabilities are determined by real properties.
(2) Actions at A can instantaneously influence properties at B.

Locality, no hidden variables

(1) Probabilities are not determined by real properties.
(2) Actions at A cannot affect B instantaneously.

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

(2) Actions at A can instantaneously influence properties at B.

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

Then why on earth can't we certify an unseeded QRNG?

(2) Actions at A can instantaneously influence properties at B.

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

Then why on earth can't we certify an unseeded QRNG?

(2) Actions at A can instantaneously influence properties at B.

But wasn't one key assumption of DI that A cannot do that?

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

Then why on earth can't we certify an unseeded QRNG?

(2) Actions at A can instantaneously influence properties at B.

But wasn't one key assumption of DI that A cannot do that?

Ahhh, you see, the precise way in which A can influence properties at B does not allow signaling.

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

Then why on earth can't we certify an unseeded QRNG?

(2) Actions at A can instantaneously influence properties at B.

But wasn't one key assumption of DI that A cannot do that?

Ahhh, you see, the precise way in which A can influence properties at B does not allow signaling.

So how can I tell what influences allow signaling?

DI QRNG assuming nonlocal hidden variables

(1) Probabilities are determined by real properties.

Then why on earth can't we certify an unseeded QRNG?

(2) Actions at A can instantaneously influence properties at B.

But wasn't one key assumption of DI that A cannot do that?

Ahhh, you see, the precise way in which A can influence properties at B does not allow signaling.

So how can I tell what influences allow signaling?

I guess you just have to learn some quantum mechanics :-)

DI QRNG assuming locality

(1) Probabilities are not determined by real properties.

(2) Actions at A cannot affect B instantaneously.

DI QRNG assuming locality

(1) Probabilities are not determined by real properties.

Hence one cannot certify an unseeded QRNG.

(2) Actions at A cannot affect B instantaneously.

DI QRNG assuming locality

(1) Probabilities are not determined by real properties.

Hence one cannot certify an unseeded QRNG.

(2) Actions at A cannot affect B instantaneously.

Hence no signaling follows for space-like separated systems.

DI QRNG assuming locality

(1) Probabilities are not determined by real properties.

Hence one cannot certify an unseeded QRNG.

(2) Actions at A cannot affect B instantaneously.

Hence no signaling follows for space-like separated systems.

From now on we assume locality and no hidden variables.

Attitudes towards the relevance of interpreting probability

Attitudes towards the relevance of interpreting probability

Physicists

stick to the fiction that it doesn't matter because thinking about it leads to uncomfortable truths. They often get away with this because they can generate large quantities of data.

Attitudes towards the relevance of interpreting probability

Physicists

stick to the fiction that it doesn't matter because thinking about it leads to uncomfortable truths. They often get away with this because they can generate large quantities of data.

Mathematicians:

"Let (X, Σ, μ) be a measure space. [...]"

Attitudes towards the relevance of interpreting probability

Physicists

stick to the fiction that it doesn't matter because thinking about it leads to uncomfortable truths. They often get away with this because they can generate large quantities of data.

Mathematicians:

"Let (X, Σ, μ) be a measure space. [...]"

Computer scientists:

On the one hand, they successfully turned the study of pseudo-randomness into a branch of mathematics (see above). On the other hand they acknowledge that they don't really know how to characterize physical sources of randomness.

Personalist probability (de Finetti, Ramsey, Savage)

Personalist probability (de Finetti, Ramsey, Savage)

- The rules of probability theory are grounded in decision theory ("how should I act").
- They have a normative character.
- They can be derived from the requirement of "no sure loss" (Dutch book coherence).

Dutch book (adapted from Wikipedia)

horse	**odds offered**				
1 2 3	even 1:2 1:3				

Dutch book (adapted from Wikipedia)

horse	**odds offered**		**amount bet**		
1	even		\$120		
2	1:2		\$80		
3	1:3		\$60		
	total		\$260		

Dutch book (adapted from Wikipedia)

horse	**odds offered**		**amount bet**	**payout if horse wins**	**net loss**
1	even		\$120	\$240	\$20
2	1:2		\$80		
3	1:3		\$60		
	total		\$260		

Dutch book (adapted from Wikipedia)

horse	**odds offered**		**amount bet**	**payout if horse wins**	**net loss**
1	even		\$120	\$240	\$20
2	1:2		\$80	\$240	\$20
3	1:3		\$60		
	total		\$260		

Dutch book (adapted from Wikipedia)

horse	**odds offered**		**amount bet**	**payout if horse wins**	**net loss**
1	even		\$120	\$240	\$20
2	1:2		\$80	\$240	\$20
3	1:3		\$60	\$240	\$20
	total		\$260		

Dutch book (adapted from Wikipedia)

horse	**odds offered**		**amount bet**	**payout if horse wins**	**net loss**
1	even		\$120	\$240	\$20
2	1:2		\$80	\$240	\$20
3	1:3		\$60	\$240	\$20
	total		\$260		

Unlike roulette, where one is certain to lose in the long run, here the bettor will lose \$20 with certainty in a single race!

Dutch book (adapted from Wikipedia)

horse	**odds offered**	**implied prob.**	**amount bet**	**payout if horse wins**	**net loss**
1	even	1/2	\$120	\$240	\$20
2	1:2	1/3	\$80	\$240	\$20
3	1:3	1/4	\$60	\$240	\$20
	total		\$260		

Unlike roulette, where one is certain to lose in the long run, here the bettor will lose \$20 with certainty in a single race!

Dutch book (adapted from Wikipedia)

horse	**odds offered**	**implied prob.**	**amount bet**	**payout if horse wins**	**net loss**
1	even	1/2	\$120	\$240	\$20
2	1:2	1/3	\$80	\$240	\$20
3	1:3	1/4	\$60	\$240	\$20
	total	13/12	\$260		

Unlike roulette, where one is certain to lose in the long run, here the bettor will lose \$20 with certainty in a single race!

Dutch book coherence

Definition

An agent's betting odds are called *Dutch book coherent* if they rule out the possibility of a Dutch book.

Dutch book coherence

Definition

An agent's betting odds are called *Dutch book coherent* if they rule out the possibility of a Dutch book.

Theorem

An agent's betting odds are Dutch book coherent if and only if they conform to the standard probability rules.

Dutch book coherence

Definition

An agent's betting odds are called *Dutch book coherent* if they rule out the possibility of a Dutch book.

Theorem

An agent's betting odds are Dutch book coherent if and only if they conform to the standard probability rules.

How should I gamble?

The Dutch-book derivation results in a theory with a normative character.

Decision theoretic probabilities are not epistemic

They are not objective, but represent an agent's degrees of belief.

They are not about knowledge, but inform action.

QBism (Chris Fuchs, arXiv.org, 2010)

In QBism, quantum states are personal judgments

QBism . . .

. . . takes *all* probabilities to be personalist Bayesian degrees of belief. This includes probabilities 0 and 1 and probabilities derived from pure quantum states.

In QBism, quantum states are personal judgments

QBism . . .

. . . takes *all* probabilities to be personalist Bayesian degrees of belief. This includes probabilities 0 and 1 and probabilities derived from pure quantum states.

- A quantum state determines probabilities through the Born rule.
- Probabilities are personal judgments of the agent who assigns them.
- HENCE: A quantum state is a personal judgment of the agent who assigns it.

In QBism, quantum states are not epistemic

Here is a slightly edited version of Adan Cabello's recent classification of quantum interpretations:

Type I ("intrinsic realism"): probabilities are determined by real properties

(Ia) ψ is a real property ("ψ-ontic")
(Ib) ψ represents knowledge about some real property ("ψ-epistemic")

Type II ("participatory realism"): probabilities are not determined by real properties

(IIa) ψ represents knowledge ("ψ-epistemic")
(IIb) ψ represents belief, informs action ("ψ-doxastic", QBism)

Recent no-go theorems assume Type I and **have no bearing on Type II.**

The Born rule

- The Born rule provides a connection between my probabilities for the outcomes of different and in general incompatible measurements.

The Born rule

- The Born rule provides a connection between my probabilities for the outcomes of different and in general incompatible measurements.
- The Born rule has normative character. "How should I gamble?"
- Unlike probability theory, which can be derived from Dutch book coherence arguments ("no sure loss!"), the Born rule is empirical. It is a statement about the character of the world.

What the Born rule is not

The usual view:

The Born rule, so the story goes, works as a setter of probabilities from something more firm or secure than probability itself, i.e., **the** quantum state.

The QBist point of view:

There is no such thing as **the** quantum state. A quantum state is always ultimately dependent on the agent's priors. There are as many quantum states for a system as there are agents interested in considering it.

Wenn schon, denn schon

"I still do not believe that the Lord God plays dice. If he had wanted to do this, then he would have done it quite thoroughly and not stopped with a plan for his gambling: In for a penny, in for a pound. Then we wouldn't have to search for laws at all."

(Einstein to F. Reiche and wife, August 15, 1942)

Laws are deterministic vs. there are no laws

The usual reading: Einstein advocates deterministic laws.

QBist reading: there are indeed no laws.

God has done it thoroughly. There are no laws of nature, not even stochastic ones. The world does not evolve according to a mechanism.

What God has provided, on the other hand, is tools for agents to navigate the world, to survive in the world.

"A quantum physicist's reading of Aquinas"

Aquinas integrates both considerations in a response that rings surprisingly modern: not only "human free will", but *the whole creation, including its material aspect, possesses a relative autonomy from God.* This autonomy is going to be the foundation for the discussion of "fortune and chance".

(Valerio Scarani, arXiv:1501.00769)

Autonomy, not intrinsic randomness

- Quantum mechanics does not determine outcome probabilities for any given physical system (e.g., an unseeded QRNG).
- Physical systems thus possess an autonomy that goes beyond the usual idea of "intrinsic randomness".
- But quantum mechanics does provide profound new relations between an agent's probability assigments, e.g., for the inputs and outputs of a DI QRNG.

Autonomy, not intrinsic randomness

- Quantum mechanics does not determine outcome probabilities for any given physical system (e.g., an unseeded QRNG).
- Physical systems thus possess an autonomy that goes beyond the usual idea of "intrinsic randomness".
- But quantum mechanics does provide profound new relations between an agent's probability assigments, e.g., for the inputs and outputs of a DI QRNG.

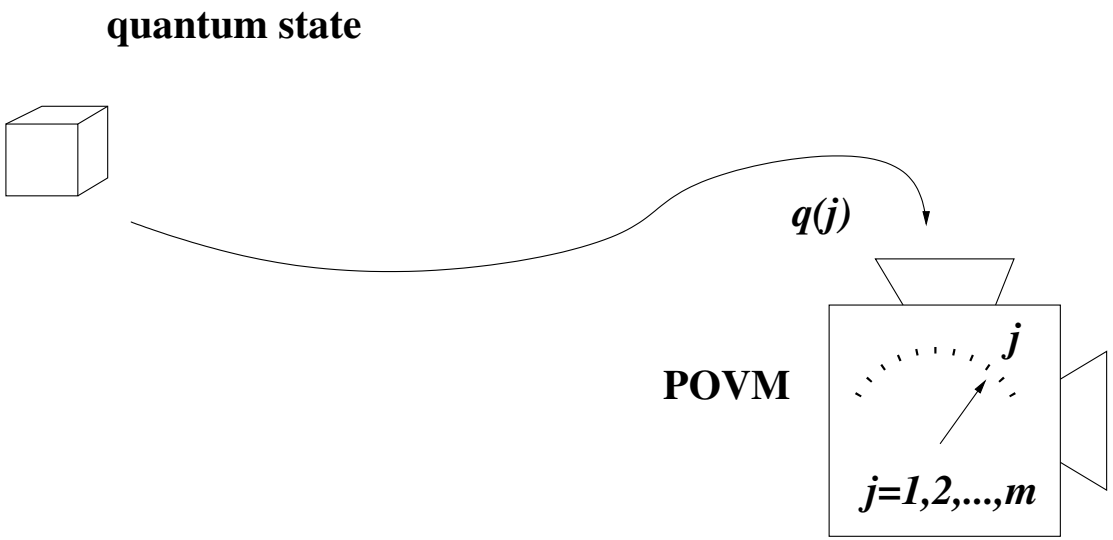
Thank you!

The End.

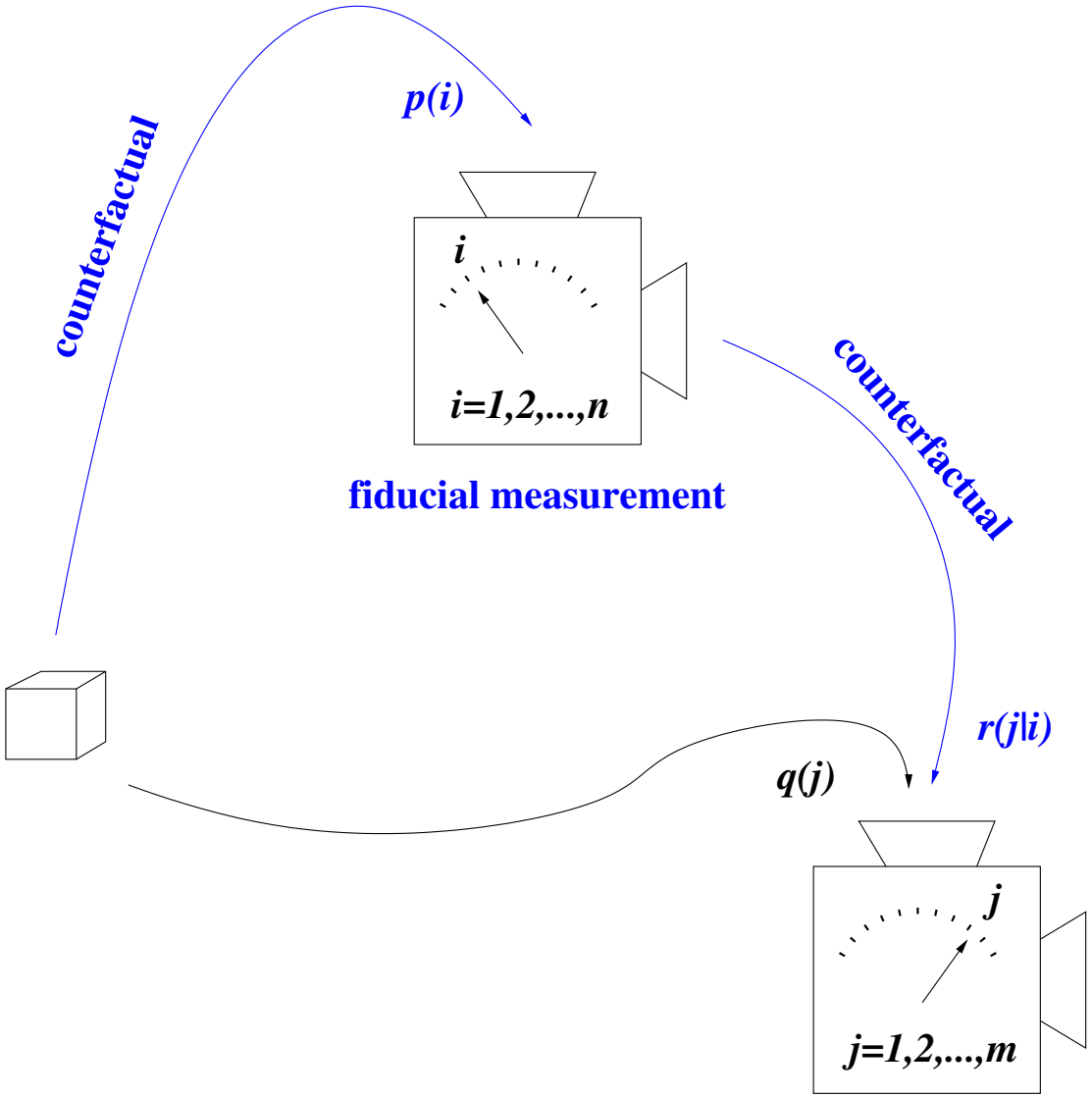
The Born rule and the double slit experiment

Born rule

$$q(j) = \mathrm{tr}(\rho E_j)$$



The Born rule and the double slit experiment



Born rule

$$q(j) = \mathrm{tr}(\rho E_j)$$

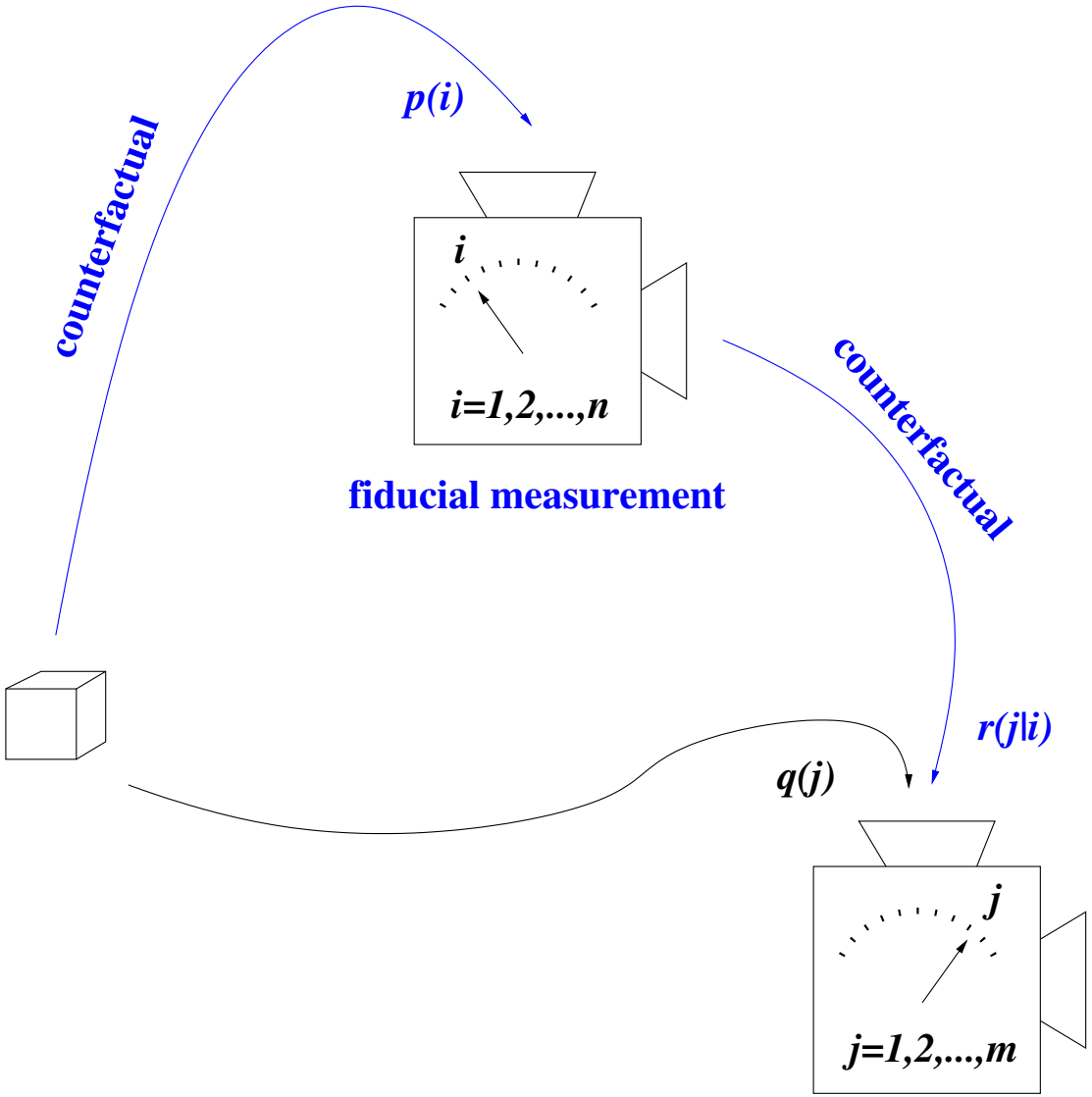
quantum state

$$\rho \longleftrightarrow p(i)$$

POVM

$$\{E_j\} \longleftrightarrow r(j|i)$$

The Born rule and the double slit experiment



Born rule

$$q(j) = \mathrm{tr}(\rho E_j)$$

quantum state

$$\rho \longleftrightarrow p(i)$$

POVM

$$\{E_j\} \longleftrightarrow r(j|i)$$

Born rule, rewritten

$$q(j) = f(p(i), r(j|i))$$