

# Can there be randomness in quantum coin tosses involving beam splitters?

<http://tph.tuwien.ac.at/~svozil/publ/2012-Paris-IHP-WOFC-pres.pdf>

<http://arxiv.org/abs/1206.6024>

Karl Svozil

University of Technology Vienna and The University of Cagliari  
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria  
[svozil@tuwien.ac.at](mailto:svozil@tuwien.ac.at)

Paris, June 28th, 2012

# Contents

## “Dogmatism as doctrine of mental reservation”

One of the most disturbing aspects of the reception of quantum mechanics by the physics community appears to be its willingness to accept incomplete knowledge *not as a challenge but as an impenetrable, irreducible dogma*.

Presently we have a situation in which it is proclaimed in one of the most venerable scientific journals by one of the most venerable physicists of our time that “the discovery that individual events are irreducibly random is probably one of the most significant findings of the twentieth century. . . . For the individual event in quantum physics, not only do we not know the cause, there is no cause.” Nowhere it is mentioned that, unlike logical, metamathematical and algorithmic undecidability, any such claim is a *belief* remaining conjectural; and that it is *provable unprovable* for the quite obvious reason that any formal proof of even lawlessness (let alone “randomness by compressed lawlessness”) would require transfinite capacities.

## “Dogmatism as doctrine of mental reservation” cntd.

I feel myself confronted with a situation which the late Ernst Specker in a personal conversation once termed a “Jesuit lie:” very often, some facts are revealed that are favourable to some party’s opinion, while other facts which are not so favourable are not mentioned at all, or remain “conveniently unmentioned.” As a consequence, misinterpretations if not erroneous perceptions abound.

## Do measurements exist?

Without measurement, the late Schrödinger once polemically noted, quantum theorists would be continuously troubled that their “surroundings rapidly turning into a quagmire, a sort of a featureless jelly or plasma, all contours becoming blurred, [they themselves] probably becoming jelly fish.” Time and again, the measurement problem has been presented and proclaimed solved in various ways, yet it pops up every now and then as remaining an open question. For the late Bell’s most quantum physicists appear to be “why bother?’ers” (cf. Dirac’s position paper) who might just as well neglect the measurement problem by considering it solved “for all practical purposes” (FAPP).

Yet, if one insists in an exact treatment of these issues, one is soon meddling with the following problem, which disturbed Wigner and Everett: *if quantum mechanics is universally valid, and if it is governed by unitary, reversible, one-to-one evolution, how does irreversibility arise from reversibility?*

## Formal aspect: 'Emergence' of many-to-one from one-to-one functions?

The formal aspect is related to question of whether it is possible to obtain an irreversible many-to-one function from reversible one-to-one (injective) functions. Pointedly stated: "how can many-to-one-ness possibly 'emerge' from one-to-one-ness?"

More specifically, as unitary (quantum) transformations (in-between measurements) are bijections, the question is if any many-to-one function (modelling the "state reduction" or the "wavefunction collapse") can be constructed from bijections.

Actually, consider the following very elementary proof by contradiction. Suppose (wrongly) a hypothetical many-to-one function  $h(x) = h(y)$  for  $x \neq y$  exists which would somehow 'emerge' from injective functions. Any such function would have to originate from the domain of one-to-one functions such that, for all functions  $f$  of this class,  $x \neq y$  implies  $f(x) \neq f(y)$  – or, equivalently, the contrapositive statement (provable by comparison of truth tables)  $f(x) = f(y)$  implies  $x = y$ , a clear contradiction with the assumption.

'Emergence' of many-to-one from one-to-one functions? -  
cntd.

No (finite) functional concatenation or injective (distinctness preserving) operation will be able to change that. Indeed, any bijection from the set of reals (or complex numbers) to the set of real (or complex) numbers is called a *permutation*. The permutation group is a group whose elements are the bijections from a given set to itself, and whose group operation is the composition of bijections. Injections form semigroups because their inverse need not exist.

Hence, I believe, that the hypothesis or believe that irreversible measurements can be reconciled with the assumption that the (unitary) quantum evolution is universally valid will eventually be identified as being what it is – an illusory *red herring*. The time when this will be acknowledged by the physics community is determined by the subjective willingness of physicists to acknowledge and not neglect an otherwise rather trivial issue.

## Empirical aspect: 'Undoing' measurements

Another, more empirical, question is: “is there a principle (and not only practical or technological FAPP) limit to ‘undoing’ measurements?”

I believe that there is none, as various quantum erasure experiments seem to indicate . And thus, what one calls “measurement,” as well as the cut between observer and object, is purely conventional. Because, as has been already argued by Wigner and Everett and alluded to earlier, even if one has located such a *Cartesian cut*, and drew the line between object and measurement apparatus, this divide is whisked away into thin air by merely considering a larger, quantized system containing both the aforementioned object and measurement apparatus.



## What constitutes a pure quantum state?

Arguably the most fundamental property of a Hilbert space is its dimension. For quantized systems, the (minimal) dimension required is the number of possible, mutually exclusive outcomes. That is, in a generalized beam splitter scenario which serves as a robust analogue of any quantized system, whenever the number of (input and output) ports is  $d$ , so is the dimension of the Hilbert space modelling that beam splitter. Operationally, in an ideal setup (no losses in the beam paths *et cetera*) one (and only one) detector, out of an array of  $d$  detectors (located after the output ports) clicks.

Any such system represents a maximal knowledge about a quantized system, which (ideally) is certain; as well as a complete control of the preparation. Here the terms “maximal” and “complete” refer to the fact that there is no operational procedure which could improve either the magnitude of definite knowledge, or the precision of the preparation.

## What constitutes a pure quantum state? -cntd.

At the same time, any such an array of  $d$  detectors can be represented by some single yet arbitrarily oriented orthonormal basis containing  $d$  orthonormal vectors in  $d$ -dimensional Hilbert space. It is therefore suggested that *a pure state is characterized by an orthonormal basis.*

Synonymously one could also define a pure state as (i) a *maximal operator* from which all commuting operators can be functionally derived, or (ii) as a *context, subalgebra* or *block*, or (iii) as a unitary transform associated with that orthonormal basis.

## The epistemic or ontic (non-)existence of mixed states

It is rather evident that FAPP all physical state preparations and measurements are incomplete and thus give rise to *epistemic uncertainties* about a prepared and measured (pure) state. An entirely different issue is whether “mixed states can be ontic;” that is, whether it is possible to “produce truly” mixed states which are not merely disguised pure states.

Again, from a purely formal point of view, it is impossible to obtain a mixed state from a pure one.

Therefore, any ontological mixed state has to be either carried through from previously existing mixed states; if they exist.

I would like to challenge anyone not convinced by the formal argument involving bijections and the permutation group to come up with a concrete experiment that would “produce” a mixed state from a pure one.

Epistemic or ontic existence of pure but entangled and/or coherent states

Basis-dependent epistemic viewpoints on a quantized system.

## The (non-)existence of quantum value indefiniteness and its purported “resolution” by quantum contextuality

The Kochen-Specker theorem, as well as other arguments (e.g. Bell- and Greenberger-Horne-Zeilinger type constructions) reveal that it is impossible for certain even finite observables to simultaneously co-exist – in such a way that (i) different observables (propositions) in the same block (state) behave classical; and (ii) everywhere in this configuration of observables (propositions), an observable occurring in some particular but arbitrary context (block, basis, subalgebra) must have precisely the same (truth) values as that same observable in different contexts. Alternatively one could say that a global consistent truth table (or value assignment) cannot exist for certain collections of observables.

## The (non-)existence of quantum value indefiniteness and its purported “resolution” by quantum contextuality

Rather than assuming the most obvious conjecture that certain observables cannot simultaneously co-exist, in the literature this is mostly interpreted as indication for *contextuality*; that is, as somehow “implying” that a certain observable may yield different outcomes, depending on what other observables are measured alongside of it. Contextuality is not present on a statistical level – a quantum operator (projector) is context independent. Rather, contextuality only “reveals” itself for individual events. Maybe this “contextual resolution” of the issues raised by Kochen and Specker and others has been the preferred hypothesis because it (i) allows one to maintain a revised realism by believing in the “existence” of observables; regardless of preparation and measurement; (ii) conforms with the experience that, any particular one of the observables occurring in the Kochen-Specker proof *can be actually “measured;” regardless of the state prepared*. That is, any such type of “measurement” results in an “answer” or “outcome.”

## The ontological single pure state conjecture

It needs, however, not be taken for granted that the outcome of a measurement reflects, or is a sole function of, the state prepared. Rather, it appears to be much more natural to assume that only in the case of a perfect match between preparation and measurement (context), the results are identical. In all other cases, the measurement apparatus, through its many degrees of freedom, might introduce a kind of “stochasticity.” But this kind of FAPP “stochasticity” is epistemic and not ontic; although it is often believed to originate from essentially nothing, in which case it must be irreducible.

I propose here what can be called the *ontological single pure state conjecture*: at any given time the system is in a definite pure state.

## Origin of Randomness through context translation

The potential infinity of (counterfactual) measurement outcomes are (i) either precisely determined in the case when there is a perfect *match* between the context or state prepared on the one hand, and the context or propositions measured on the other hand; (ii) or, in the case of a context mismatch, epistemic stochasticity enters through the environment (measuring apparatus) translating between the information prepared and the question asked. This could, at least in principle, be tested by changing the capability of the environment to translate contexts.



## Is the best interpretation of the quantum formalism its non-interpretation?

Time and again, the quantum theorist is reminded by prestigious peers that the best interpretation of quantum mechanics appears to be its non-interpretation. Indeed, as has been pointed out earlier, it has become almost fashionable to discredit interpretation and causality in the quantum domain. Already Sommerfeld warned his students not to get into these issues, and not long ago scientists working in that field have had a hard time not to appear as “quacks.”

We are confronted with a situation in which an orthodoxy tries to suppress and avoid thinking about the “how,” or at least advises “not worry too much,” while at the same time expressing the opinion that certain events occur *ex nihilo* (out of nothing), fundamentally inexplicably, and irreducibly random. This, I believe, is tantamount to dogmatism, and contradictory to all rationalistic principles on which scientific progress thrives.

## Quantum random number generators

Although, as has been mentioned earlier, quantum randomness, or at least Turing incomputability from quantum coin tosses involving beam splitters, is often judged to be the “ultimate” randomness, and even “the (nihilistic) message of the quantum,” some questions with regard to the conceptual foundations arise. For instance, an ideal beam splitter can be modelled by a unitary transformation, which is a (Laplacian type causal) one-to-one isometric transformation in Hilbert space.

No information is lost in such devices, which are (at least ideally) incapable of irreversibility. Operationally this can be demonstrated by the serial composition of two beam splitters, which effectively renders a Mach-Zehnder interferometer yielding the original quantum state in its output ports. One may say that the “randomness resides” in the (classical) detection of, say, the photons, after the half-silvered mirror.

## Quantum random number generators cntd.

But, as has for instance been pointed out by Everett, this is (self-)delusional, as quantum mechanics, and in particular the unitary quantum evolution of all components involved in the detection, at least in principle must hold uniformly.

The situation discussed is also related to the issue of “quantum jellification” posed by the late Schrödinger with regards to the coherent superposition and co-existence of classically contradictory physical states. But how can irreversibility possibly “emerge” from irreversibility? Besides "for-all-practical-purposes" being effectively irreversible, in principle there does not seem to exist any conceivable unitary route to irreversibility; at least if quantum theory is universally valid.

## Quantum random number generators cntd.

Thus, in view of a causal, bijective Laplacian type quantum evolution, what guarantees a quantum coin toss, say, on a half-silvered mirror, to perform irreducibly random, and where exactly does this randomness originate? The issues appear as marred today as in Wigner's times, but they are much more pressing now, as the associated technologies have been deployed for experiments as well as cryptanalysis and industry by various spin-offs.

## Quantum random number generators cntd.

One possibility to circumvent this conundrum is by postulating (i) that at every instant, only a single state (or context) exists; and (ii) through *context translation*, in which a mismatch between the preparation and the measurement results in the “translation” of the original information encoded by a quantum system into the answer requested, noise is introduced by the many degrees of freedom of a suitable “quasi-classical” measurement apparatus. But this would be an altogether different source of randomness than irreducibly creation *ex nihilo* (“out of nothing”) that is favoured by the present quantum orthodoxy.

Thank you for your attention!

