Randomness, Indeterminism, and Unpredictability in Quantum Mechanics

Alastair A. Abbott

Institut Néel (CNRS & Université Grenoble Alpes), Grenoble, France

Grenoble, 29 mars 2017

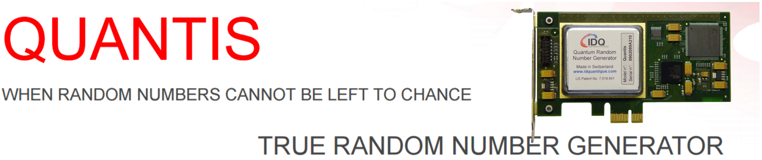
Randomness and Quantum Mechanics

Since the formative years of quantum mechanics, randomness has been understood to have a crucial role at the heart of the theory

- Considered key to properly understanding quantum mechanics

More recently, quantum randomness harnessed to play a central role in some quantum technologies

- Viewed as inherently different in nature from, and superior to other types of randomness



What is (Quantum) Randomness?

But what *is* randomness, and in what sense does quantum randomness really differ from other types of randomness?

- Many delicate connections with concepts of chance, indeterminism and unpredictability

"*The predictions of quantum mechanics are intrinsically probabilistic and random! Accepting quantum mechanics means making an assumption that it is correct, and consequently intrinsically random.*"[1]

"*Any classical system admits in principle a deterministic description and thus appears random to us as a consequence of a lack of knowledge about its fundamental description. Quantum theory is, on the other hand, fundamentally random.*"[2]

[1] M. Bera *et al.*, arXiv:1611.02176, 2016.

[2] S. Pironio *et al.*, Nature 464 (2010), p. 1021.

Outline

Quantum Measurement and Indeterminism
- Quantum measurement and the Born rule
- Bell-Kochen-Specker Theorems and quantum indeterminism

Randomness, Chance & Indeterminism
- Three subtle, related concepts
- Randomness as unpredictability

Unpredictability and Randomness
- Formalising unpredictability
- Quantum randomness

Quantum Random Number Generators

Elements of Quantum Theory

- States are represented by unit vectors in a complex vector space
  - Can be associated to "sure" properties of system, e.g. $|S_z = +\rangle$
  - Superposition: $|S_x = +\rangle = \frac{1}{\sqrt{2}}\big(\,|S_z = +\rangle + |S_z = -\rangle\,\big)$
- Observables are Hermitian operators corresponding to sets of mutually exclusive "propositions" (called contexts)
  - e.g. $S_z = \sum_{\pm} \pm|S_z = \pm\rangle\langle S_z = \pm|$
  - State only specifies measurement outcome with certainty if $A\,|\psi\rangle = a\,|\psi\rangle$
  - Measurements disturb the system if the state is not an eigenstate of the measured observable
  - Observable properties are generally not simultaneously measurable: $[S_z, S_x] \neq 0$
- Dynamics are unitary and reversible
  - Conflict with measurement: the *measurement problem*

The Born Rule

The Born rule links the abstract quantum state to the concrete observation of outcomes

The Born rule

The probability of observing outcome a_i upon measurement of the context $\{|a_i\rangle\langle a_i|\}_i$ on a state $|\psi\rangle$ is $p(a_i|\psi) = |\langle a_i|\psi\rangle|^2$. Following the observation of outcome a_i, the system "collapses" to the state $|a_i\rangle$.

- This rule only tells us how to assign probabilities to observations, but is silent towards its physical *interpretation*
  - Although the theory is intrinsically *probabilistic*, this alone is well short of any conclusion of intrinsic *randomness*
- Nor does it say anything about how this state collapse occurs

Interpreting the Born Rule

Epistemic interpretation

- The probabilities express only our ignorance as to the true physical state of the system, and statements about the quantum state should be interpreted as referring to physical ensembles
  - Einstein & Schrödinger notably favoured such an approach
  - "*The statistical interpretation due to Born . . . allows, however, no real description for the individual system, rather only statistical assertions concerning ensembles of systems.*" (Einstein, 1953)

Ontic interpretation

- The probabilities must be interpreted as physical propensities, and thus quantum measurement is fundamentally chancy and indeterministic
  - "*I myself tend to give up determinism in the atomic world.*" (Born, 1926)

Interpreting the Born Rule (2)

This ontic interpretation has become predominant, particularly in the modern information-theoretic approach to QM

Eigenstate–Eigenvalue Link[3]

A system in a state $|\psi\rangle$ has a definite value of an observable property A if and only if $|\psi\rangle$ is an eigenstate of A.

- This interpretation represents a radical departure from classical determinism; what basis do we have for believing this is necessary?
- And does this interpretation entail the randomness of measurement outcomes?
  - Need to look at *what* randomness is and how it's related to indeterminism

[3] M. Suárez, Br. J. Phil. Sci. 55 (2004), p. 222.

Hidden-Variable Theories

In the 1960s, following earlier work by von Neumann, Bell and, simultaneously, Kochen and Specker, asked whether an epistemic interpretation of the Born rule is really tenable

A hidden variable theory posits a hidden parameter λ completely determining the observable properties of the system:

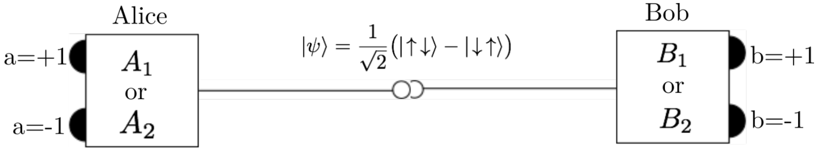
- Preparation of $|\psi\rangle$ corresponds to preparing a state $\lambda \in \Lambda_\psi$ completely determining all measurement outcomes
- The Born rule is recovered as an ensemble average

Bohmian mechanics shows a hidden variable account of quantum mechanics possible, but Bell, Kochen and Specker showed that such theories can be excluded under extra, seemingly reasonable, physical assumptions

Bell's Theorem and Inequalities

Bell showed that any local hidden variable theory must produce correlations that satisfy certain "Bell inqualities"

- Locality: The measurement outcomes are a function only of λ and the *local*, freely made, measurement choice



$$\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle \leq 2$$

- Quantum theory predicts violation of these inequalities, and experiments confirm concur
- The derivation is *independent* of quantum mechanics

The Kochen-Specker Theorem

Kochen and Specker showed that the contradiction with determinism occurs for individual particles, *prior* to measurement, and *independently of the state*

Kochen-Specker Theorem (strengthened)

Let $|\psi\rangle$ be any state and $A = \sum_i a_i |a_i\rangle\langle a_i|$ an observable. Then the outcome of a measurement of A can be pre-determined non-contextually if and only if $|\psi\rangle = |a_i\rangle$ for some i.

- Noncontextuality generalises locality by requiring that if the outcome of a measurement A is predetermined, the outcome should be independent of any compatible observable B also measured

Bell and KS theorems justify the E-E link by proving indeterminism under weak assumptions about how deterministic theories must be

Is Randomness Indeterminism?

Does quantum indeterminism amount to quantum randomness? More generally, can randomness be equated with indeterminism?

- Many claims of quantum randomness indeed appeal to indeterminism

"*The result is completely random because in such a measurement the elementary system carries no information whatsoever about the measurement result.*"[4]

"*A crucial question in physics (and even philosophy) is whether nature is deterministic or intrinsically random.*"[5]

- Until recently, the concepts of indeterminism, randomness, and *(objective) chance* were often identified within the philosophical literature

[4] A. Zeilinger, Found. Phys 29 (1999), p. 636.

[5] A. Acín, in *Is Science Compatible with Free Will?* (2003), p. 7.

Physical Indeterminism

"*Une intelligence qui, à un instant donné, connaîtrait toutes les forces dont la nature est animée et la situation respective des êtres qui la composent, si d'ailleurs elle était suffisamment vaste pour soumettre ces données à l'analyse, embrasserait dans la même formule les mouvements des plus grands corps de l'univers et ceux du plus léger atome ; rien ne serait incertain pour elle, et l'avenir, comme le passé, serait présent à ses yeux.*" (Laplace, 1814)

Indeterminism is defined as the logical negation of determinism

Determinism (Earman, Montague)

A theory is deterministic if the state of a (closed) system at time t_0 uniquely determines its future state for all $t > t_0$.

Indeterminism, Chance and Randomness

It is instructive to analyse this identification in two parts:

(IC) Something happens by chance iff it is indeterministic

(CT) Something is random iff it happens by chance

What is meant by '(objective) chance'?[6]

- Refers to possibility (as opposed to necessity);
  Leibniz: "*probabilitas est gradus possibilitas*"
- Has a quantitative aspect, representable as probabilities
- Regulates rational belief in line with Lewis' Principal Principle:

$$\mathsf{Cr}(A|\text{``}P(A|E) = x\text{''} \wedge E) = x$$

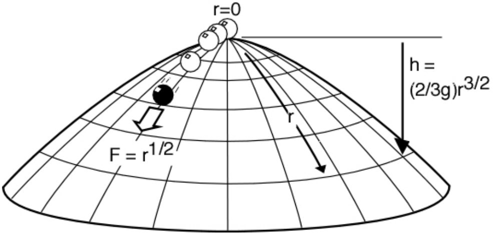
- Should relate to frequency of realisation in similar circumstances

[6] E.g. J. Schaffer, Brit. J. Phil. Sci 54 (2003), 27–41; D. Mellor, Aus. J. Phil. 78 (2000), 16–27.

IC: Indeterminism and Chance

IC has been challenged in several ways in recent years

- Arguments for deterministic chance, mostly based on existence of probabilities that objectively play the role of chance in theories despite underlying determinism[7]
- Indeterminism in (even classical) physics that doesn't play the role of chance, e.g. Norton's dome



[7] Eg. B. Loewer, Stud. Hist. Phil. Mod. Phys. 32 (2001), pp. 609–620; Eagle, Noûs 45:2 (2011), 269–299.

Quantum Measurement and Chance

The negative definition of indeterminism leaves the future "*completely unspecified. [...] Randomness such as described by the Born rule of quantum mechanics, on the other hand, is not a matter of 'anything goes', but a highly constrained affair: exactly one of a number of possible outcomes will occur, and the probabilities of all the outcomes are given beforehand.*"[8]

- So quantum measurements seems to fit the bill for being considered (objectively) chancy

Müller goes on to argue that quantum randomness is precisely this kind of constrained indeterminism

- This argument, and other more casual ones, for quantum randomness nonetheless appeal implicitly to the CT

[8] T. Müller, *(Quantum) randomness as limited indeterminism* (2015).

The Commonplace Thesis

(CT) Something is random iff it happens by chance

For CT to be tenable, chance needs to satisfy what we expect of randomness

The qualities of randomness can be divided into two groups: those dealing with objects, and those dealing with processes

- Product randomness: is a particular sequence of results of coin flips random?
- Process randomness: is the coin-flip process random?
- Chance is clearly a process notion, so already clear that the CT can only directly apply to a process notion of randomness

Product Randomness

The notion of randomness for finite and infinite sequences has been rigorously formalised as a form of disorder or patternlessness

$$0101010101010101010101010101010101010101$$
$$0100011011000001010011100101110111000000$$
$$0001000000010000101001110111000011111010$$

- Borel and von Mises made important historic contributions
- Not sufficient to demand the uniformity of bits, as Champernowne's number shows
- Can we call a sequence random if it contains no patterns at all? Martin-Löf and Kolmogorov independently showed that such a notion is vacuous: such absolute randomness is mathematically impossible

Algorithmic Randomness Randomness

Kolmogorov (1965), Martin-Löf (1966), Chaitin (1966) showed how randomness can rigorously be defined using computability theory

- A sequence is random if contains no *computably detectable* patterns
  - Equivalently, it is *incompressible*
  - Robust in the infinite limit, but some problems applying it to (short) finite string, and particular *individual* outcomes
  - It is impossible to determine (i.e., incomputable) whether a given sequence is random or not

Algorithmic randomness nonetheless robust and corresponds well to many intuitions about randomness and its scientific use in many contexts

Process Randomness

Less consensus, but often seen as related to unpredictability

- Idea already present in Laplacian indeterminism, and taken up by others including Popper[9]
    - Need to be able to talk about individual random events
- Eagle goes a step further defined randomness as "maximal unpredictability"

Defining randomness as a form of unpredictability identifies a subjective element in randomness: unpredictable for whom? And under what conditions?

Many paradigmatic random events are (at least partially) deterministic:

- Coin tossing, trajectories of chaotic systems

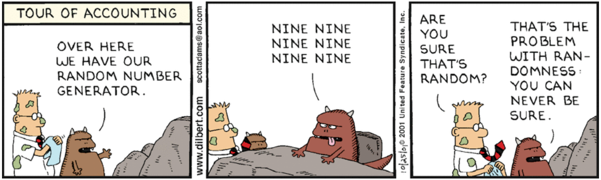
---

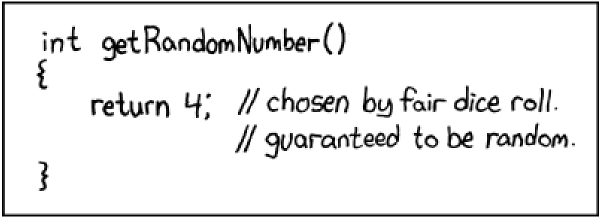
[9] Br. J. Phil. Sci, 1 (1950), 117.

One Randomness to Rule Them All?

Both product and process randomness seem legitimate and fruitful notions

- Could we nonetheless hope to unite them?





The Commonplace Thesis Debunked

Eagle (and others) have argued at length that the CT is problematic even for process randomness

- Deterministic randomness a key counterexample
- Randomness seems to have at least some subjective component that chance does not

Accounts of quantum randomness *as* indeterminism or objective chance thus seem to fall short, and unpredictability seems a better explanatory tool

- Indeed, some recent accounts have appealed to unpredictability

"*An immediate consequence of this is objective randomness. [...] we can in principle only make a probabilistic prediction of, say, the position of a particle in a future measurement.*"[10]

[10] J. Kofler & A. Zeilinger. Eur. Rev. 18 (2010), p. 470.

Randomness as Unpredictability

To make the connection more robust, we need to formalise more carefully what it means for a process to be unpredictable

- We want a notion that is sensitive to different forms or strengths of unpredictability and randomness

Central to most such attempts is an agent or "predictor" who must make predictions

- This formalises the subjective component of unpredictability, but note that this does not mean unpredictability isn't intrinsic, or that it can't have an objective origin
- This subjective aspect must be reconciled with the supposedly "absolute" nature of quantum randomness

Not clear whether unpredictability should require *uniformity*

Formalising Unpredictability

How can we formalise what it means for an event to be predictable?

- Laplace's "*intelligence qui ... connaîtrait toutes les forces dont la nature est animée et la situation respective des êtres qui la composent, si d'ailleurs elle était suffisamment vaste pour soumettre ces données à l'analyse*" is hardly physical
- Popper attempted to effectivise such an agent, requiring it to act via physical means and with finite precision[11]
- Eagle considered a subjective model in which an agent – operating with a given theory and epistemic means – makes predictions that they use as their posterior credence[12]
  - The most serious attempt, but too subjective to compare quantum and classical randomness well

[11] K. Popper, Br. J. Phil. Sci. 1 (1950), 118,124.

[12] A. Eagle. Brit. J. Phil. Sci. 56 (2005), 749.

An Effective Model of Unpredictability

We propose a model[13] that:

- Is explicitly *effective*: the predictor must make a prediction using *computable, finite means*
- The predictor uses *finite information extracted locally* from the physical system *via measurement* to compute a prediction

More precisely, for an experiment/prediction task E, consider

- An extraction technique ξ used to obtain *finite, locally accessible* information $\xi(\lambda)$ from the ontological state λ
- A computable function P_E which computes a prediction using the information extracted: i.e. $P_E(\xi(\lambda))$
- E is ξ-predictable if there exists a P_E such that, for any instantiation of E, the prediction $P_E(\xi(\lambda_i))$ is always correct
- E is predictable if there exists a ξ such that it is ξ-predictable

[13] A. Abbott, C. Calude & K. Svozil, Information 6 (2015), 773.

An Effective Model of Unpredictability

Weak Randomness

An experiment E is Ξ-random or *(Ξ-)weakly random* if it is ξ-unpredictable for any $\xi \in \Xi$.

Strong Randomness

An experiment E is *strongly random* iff it is ξ-unpredictable for any ξ.

The degree of subjectivity can be varied by changing the epistemic capabilities of the predictor

- An absolute notion is obtained in the limit
- Even if a prediction is subjective (i.e., made by a particular predictor), unpredictability can be objective in the sense that an event is unpredictable for *any* predictor with such means

Quantum Randomness

How does quantum randomness fare under this notion of "randomness as unpredictability"? And how does it compare to classical randomness?

- It is not difficult to show that (quantum) indeterminism implies unpredictability and strong randomness
    - λ doesn't determine, and thus can't be used to predict, the measurement outcome

Quantum measurements are therefore random in the strongest sense

More generally, we see that chance and indeterminism are sufficient, but not necessary causes of randomness

$$\text{Chance} \implies \text{Indeterminism} \implies \text{Randomness}$$

Chaotic Randomness

What about classical chaotic systems?

"Il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux; une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible."[14]

- Given a class Ξ of extractors with bounded precision, such systems can produce weakly random events
  - Not strongly random assuming classical mechanics, since a sufficiently good extractor exists for any E
  - If such a limit represents a fundamental physical restriction, would be strongly random
  - For such systems, external perturbations pose a further, eventually more important, limit

Thus, in principle, one may have deterministic, intrinsic randomness

[14] H. Poincaré, Science et Methode, Flammarion (1908), 68–69.

Quantum vs Classical Randomness

Thus, although quantum randomness is indeed absolute, the key difference to classical randomness is the degree of objectivity

- Deterministic randomness can be intrinsic too, and even, in principle, just as unpredictable
- While quantum indeterminism may be the origin of quantum randomness, it is not *a priori* what makes it stronger than classical randomness

In Bell-type scenarios, if the parties have free choice of their inputs, a violation of a Bell-inequality implies strong unpredictability irrespective of whether determinism holds, as long as "no-signalling" is obeyed

- Quantum randomness is present even in more modern *epistemic* interpretations of quantum mechanics

Random Number Generators

Random number generators (RNGs) play an essential role in simulation, probabilistic algorithms, cryptography, etc.

- RNGs aim not only to be unpredictable, but to be a uniformly distributed source of bits
- PseudoRNGs are widespread, even if their shortcomings well known

"Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. [...] there is no such thing as a random number – there are only methods to produce random numbers" (von Neumann)

- Quantum randomness seems ideally suited to this task

Product/Process Uneasiness

It is nonetheless often convenient (and common) to conflate the randomness of a RNG and that of its (generic) output

- In practice, only the output is testable, and need to try and quantify the randomness
  - Typically, the entropy of the source is estimated from the observed statistics and measured in *bits*
  - Will only overstate the true randomness, perhaps dramatically

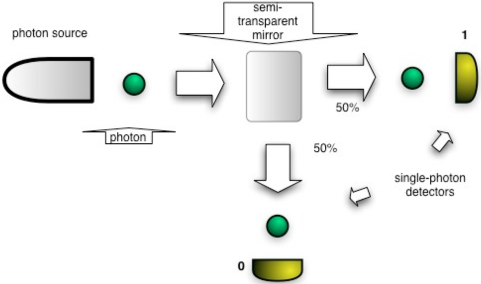
In some applications, such as cryptography, both product *and* process randomness desirable, while formal results consider only probability distributions

- Need to be careful draw unjustified conclusion by mixing the two concepts

E.g., *"Unfortunately computers are not able to generate true random numbers, as they are deterministic systems."*

Quantum RNGs

- First proposals based on radioactive decay
- Archetypical modern example is a simple beamsplitter



- Other methods include photon time-of-arrival measurements
- QRNGs capable of fast (10Mbit–1Gbit) generation of high quality randomness

QRNGs vs Classical RNGs

The superiority of quantum randomness over classical randomness is a major selling point for QRNGs

- Clear benefit over pseudoRNGs, where all the unpredictability is in the initial seed
- Our analysis of quantum randomness highlights unpredictability, not indeterminism, as the key advantage

What about chaotic randomness?

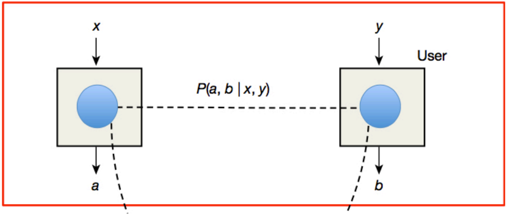
- In a trusted setting, such a device should provide randomness that is just as unpredictable to an observer
- The *simplicity* of QRNGs is crucial: easier to model, control, and understand the source of randomness
  - Classical randomness arises out of complexity, rather than simplicity

Device Independent QRNGs

In cryptography, unpredictability from potential adversaries is precisely what is needed, and for this we may not want to trust our QRNG

Bell-inequality violation can be used to certify unpredictability, and thus the quality of a QRNG

- Requires that the inputs uncorrelated from the device and any adversary
  - Thus, “device-independent” QRNGs are actually randomness expanders, transforming a small seed $p(xy)$ into a device generating many more bits



A. Acín & L. Masanes. Nature 540 (2016), 213.

Summary

- Accounts of quantum randomness have generally been based on quantum indeterminism and invoked the Commonplace Thesis to deem measurements random
- The process notion of randomness applicable to individual quantum measurements can be formalised rigorously via lack of effective (i.e. computable) predictability
- This approach highlights degree of objective unpredictability as the factor distinguishing quantum and classical randomness, rather than indeterminism *per se* or its intrinsic nature
- An improved awareness of the distinction between product and process randomness, as well as the notions of indeterminism, randomness and unpredictability can hopefully help to better develop systems based on quantum randomness and understand their benefits

References

- A. A. Abbott, C. S. Calude and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness. *Journal of Mathematical Physics*, 56:102201, 2015.
- A. A. Abbott, C. S. Calude and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6:773, 2015.
- J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.
- M. N. Bera, A. Acín, M. Kus, M. Mitchell and M. Lewenstein. Randomness in Quantum Mechanics: Philosophy, Physics and Technology. arXiv:1611.02176 [quant-ph], 2016.
- J. Bub. The Measurement Problem from the Perspective of an Information-Theoretic Interpretation of Quantum Mechanics. *Entropy*, 17:7374, 2015.
- A. Eagle. Randomness is Unpredictability. *British Journal for the Philosophy of Science*, 56:749, 2005.

References (2)

- G. Jaeger. Quantum randomness and unpredictability. *Fortschritte der Physik*, 2016.
- S. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59, 1967.
- J. Kofler and A. Zeiliner. Quantum Information and Randomness. *European Review*, 18:468, 2010.
- S. Pironio et al. Random numbers certified by Bell's theorem. *Nature*, 464:1021, 2010.
- K. Popper. Indeterminism in quantum physics and in classical phyiscs. Part I and II. *British Journal for the Philosophy of Science*, 1:117, 1950.