On the unpredictability of individual quantum measurement outcomes

Alastair A. Abbott,[1,2,*] Cristian S. Calude,[1,†] and Karl Svozil[3,1,‡]

[1]*Department of Computer Science, University of Auckland,*
Private Bag 92019, Auckland, New Zealand

[2]*Centre Cavaillès, CIRPHLES, École Normale Supérieure, 29 rue d'Ulm, 75005 Paris, France*

[3]*Institute for Theoretical Physics, Vienna University of Technology,*
Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria

(Dated: July 3, 2014)

Abstract

Suppose we prepare a quantum in a pure state corresponding to a unit vector in Hilbert space. Choose an observable property of this quantum corresponding to a projector whose respective linear subspace is neither collinear nor orthogonal with respect to the pure state vector. Recent results can be then used to *prove* that this observable property has no predetermined value, and thus remains value indefinite.

As a consequence, we *prove* that the outcome of a measurement of such a property is *unpredictable* with respect to a very general model of prediction here developed.

These results are true relative to three assumptions, namely compatibility with quantum mechanical predictions, noncontextuality, and the value definiteness of observables corresponding to the preparation basis of a quantum state. This framework allows for the first time a rigorous proof of the unpredictability of some individual quantum measurement outcomes, a fact postulated or claimed for a long time.

Finally, unpredictability will be used to discuss quantum randomness—shown to be "maximally incomputable"—as well as *real* model hypercomputation whose computational power has yet to be determined.

[*] a.abbott@auckland.ac.nz; http://www.cs.auckland.ac.nz/˜aabb009

[†] cristian@cs.auckland.ac.nz; http://www.cs.auckland.ac.nz/˜cristian

[‡] svozil@tuwien.ac.at; http://tph.tuwien.ac.at/˜svozil

I. INTRODUCTION

Indeterminism has had a role at the heart of quantum mechanics since Born postulated that the modulus-squared of the wave function should be interpreted as a probability density that, unlike in classical statistical physics [1], expresses fundamental, irreducible indeterminism [2]. In Born's own words, "*I myself am inclined to give up determinism in the world of atoms.*" The nature of individual measurement outcomes in quantum mechanics was, for a period, a subject of much debate. Einstein famously dissented, stating his belief that [3, p. 204] "*He does not throw dice.*" Nonetheless, over time the conjecture that measurement outcomes are themselves fundamentally indeterministic became the quantum orthodoxy [4].

Accompanying the belief of quantum indeterminism is the view that quantum measurement outcomes are unpredictable and random [4], a view that, at least to some extent, seems intuitively to follow from indeterminism. These are all, however, subtle concepts and any such argument would be clarified immensely by formalising the situation. This has happened with indeterminism, which has progressively been formalised as value indefiniteness in the development of the theorems of Bell [5] and, particularly, Kochen-Specker [6]. These theorems, which have also been experimentally tested via the violation of various inequalities [7], express the impossibility of certain classes of deterministic theories.

While these results have given a better grounding to the belief in quantum indeterminism, it is crucial to recognise their limits. Firstly, it is important to remember that the deduction of indeterminism from these no-go theorems rests on the reluctance to accept non-classical alternatives such as nonlocality and contextual determinism, assumptions whose validity continues to be tested and analysed. Secondly, in order to understand clearly the consequences of indeterminism for unpredictability and randomness, formal notions of these concepts also need to be specified and analysed. Such notions are by no means simple to define, and we should be cautious of any attempt to assert that randomness and unpredictability follow trivially.

In this paper we systematically approach these issues. We first discuss various possible proposed notions of prediction, before presenting an objective, non-probabilistic formal model of prediction which we argue captures the notion of an 'in principle' predictable physical event or sequence thereof. We show that individual quantum measurement outcomes are unpredictable with respect to this model, confirming the intuition. The use of clear formal models allows us to identify Kochen-Specker type value indefiniteness [8] as the key reason for this unpredictability. We further discuss the issue of quantum randomness from the viewpoint of the derived unpredictability.

II. VALUE INDEFINITENESS

A. A formal basis for indeterminism

The generally accepted phenomenon of quantum indeterminism cannot be deduced from the Hilbert space formalism of quantum mechanics alone, as this specifies only the probability distribution for a given measurement which in itself need not indicate intrinsic indeterminism. Instead, it enters at the interpretational level, even if its acceptance is influenced by the analysis of no-go theorems. While we could, in our effort to clarify and formalise unpredictability, restrict ourselves to a particular interpretation, it is preferable to work from a formal definition of value-indefiniteness which represents indeterminism in a general framework [8]. Here we will briefly review this formalism, as well as the Kochen-Specker theorem which is the primary motivation for its acceptance.

For a given quantum system, we can represent the measurement outcomes which are pre-determined by a value assignment function. This partial function assigns (potentially hidden) values to those observables for which measurement results are pre-determined, which we call *value definite* observables, and may be undefined for some (or all) observables. Such *value indefiniteness* corresponds to the indeterminism of a measurement outcome.

While one could potentially hypothesise that all observables are value indefinite under the value assignment function for quantum systems, it seems that at least some conditions for value definiteness need to be respected. With respect to when we should conclude that a physical quantity is value definite, Einstein, Podolsky and Rosen (EPR) define *physical reality* in terms of certainty and predictability in [9, p. 777]. While we have not yet given a definition of predictability, we posit that any reasonable definition should render the following "EPR principle" true, which identifies their notion of an "element of physical reality" with "value definiteness":

> *EPR principle*: If, without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists a *definite value* prior to observation corresponding to this physical quantity.

We briefly note that the constraint that prediction acts "without in any way disturbing a system" is perhaps nontrivial [10], but nonetheless appears a reasonable requirement for prediction, especially in order to imply pre-determined values.

With this in mind, it seems that as a minimum requirement, the *eigenstate principle* should hold: if a quantum system is prepared in a state $|\psi\rangle$, then the projection observable $P_\psi = |\psi\rangle\langle\psi|$ is value definite. This is similar, although weaker (as only one direction of the implication is asserted) than the eigenstate-eigenvalue link [11].

We recall that a context is a set of mutually commuting observables. A further requirement that seems unavoidable is that, if some observables in a context are value definite, then if quantum mechanical identities uniquely identify the outcome for other observables in the context, they must be value definite as well. We call this *admissibility* of the value assignment function, and appears necessary to avoid measurement results that should be impossible to obtain. Note that we require this to hold only when any indeterminism (which implies multiple possible outcomes) would allow quantum mechanical predictions to be broken. As an example, given a set $\{P_1,\dots,P_n\}$ of commuting projection observables, if P_1 were to have the definite value 1, all other observables in this set must have the value 0. Were this not the case, there would be a possibility to obtain the value 1 for more than one compatible projection observable, a direct contradiction of the quantum predictions.

The Kochen-Specker theorem [6] shows that no value assignment function can consistently make *all* observables value definite while maintaining the requirement that the values are assigned non-contextually—that is, the value of an observable is the same in each context it is in. This is a global property: non-contextuality is incompatible with *all* observables being value definite. However, it is possible to localise value indefiniteness and show that even the existence of two non-compatible value definite observables is in contradiction with admissibility and the requirement that any value definite observables behave non-contextuality, without requiring that all observables be value definite.

Theorem 1 (From [8, 12])**.** *Let there be a quantum system prepared in the state $|\psi\rangle$ in dimension $n \geq 3$ Hilbert space $\mathbb{C}^n$, and let $|\phi\rangle$ be any state neither orthogonal nor parallel to $|\psi\rangle$, i.e. $0 < |\langle\psi|\phi\rangle| < 1$. Then the projection observable $P_\phi = |\phi\rangle\langle\phi|$ is value indefinite under any non-contextual admissible assignment function.*

Hence, accepting that definite values, *should they exist* for certain observables, behave non-contextually is in fact enough to derive rather than postulate quantum value indefiniteness.

B. Contextual alternatives

It is worth keeping in mind that, while indeterminism is often treated as an assumption or aspect of the orthodox viewpoint [2, 4], this usually rests implicitly on the deeper assumptions we have mentioned that the Kochen-Specker theorem relies on. If these assumptions are violated, deterministic theories could not be excluded, and the assumption of indeterminism would appear much blinder.

If this were the case, perhaps the simplest alternative would be the explicit assumption of the context dependant value definiteness, and most attempts to interpret quantum mechanics deterministically, such as Bohmian mechanics [13], can be expressed in this framework. An important caveat is that, due to the experimental verification of Bell inequalities [7], any such deterministic hidden parameters must be explicitly nonlocal. In such a theory unpredictability seems less evident as the *ex nihilo* results are sacrificed. However, predictability is still not an immediate consequence, as such hidden variables could potentially be "assigned" by a demon operating beyond the limits of any predicting agent (e.g. uncomputably).

A second alternative would be to challenge the nontrivial assumption that a predetermined outcome (corresponding to a value definite property) needs to be a deterministic function of the observable alone. Instead one could insist that the *"… result of an observation may reasonably depend not only on the state of the system … but also on the complete disposition of the apparatus"* [5, Sec. 5]. In particular this would apply to the situation of a mismatch between preparation and measurement for which the states prepared and measured are complementary (that is, neither collinear nor orthogonal).

In this viewpoint, even when the macroscopic measurement apparatuses are still idealised as being perfect, their many degrees of freedom (which may by far exceed Avogadro's or Loschmidt's constants) contribute to any measurement of the single quantum. Most of these degrees of freedom might be totally uncontrollable by the experimenter, and may result in an *epistemic uncertainty* which is dominated by the combined complexities of interactions between the single quantum measured and the (macroscopic) measurement device producing the outcome.

In such a measurement, the pure single quantum and the apparatus would become entangled. In the absence of one-to-one uniqueness between the macroscopic states of the measurement apparatus and the quantum, any measurement would amount to a partial trace resulting in a mixed state of the apparatus, and thus to uncertainty and unpredictability of the readout.

In this minority view, just as for irreversibility in classical statistical mechanics [1], the indeterminism of single quantum measurements might not be irreducible at all, but an expression of, and relative to, the limited means available to analyse the situation. In Bell's terms, the outcome may be irreversible *for all practical purposes* [14].

C. Unpredictability of individual measurements

While we wish to formalise and analyse quantum unpredictability carefully, we wish to outline carefully the intuitive reasoning first, as this should guide our approach at formalisation.

The EPR principle renders a definition of value definiteness and physical reality based on the ability to predict. Thus, it seems conversely that *value indefiniteness* corresponds to the *absence of physical reality*; if no unique element of physical reality corresponding to a particular physical quantity exists, this is reflected by the physical quantity being value indefinite. That is, for such an observable neither of the two exclusive measurement outcomes $\{0,1\}$ is certain to occur and therefore we should conclude that any kind of prediction of the outcome with certainty cannot exist, and the outcome of this individual measurement must thus be unpredictable. One possible interpretation of this unpredictability is that the physical property measured is logically independent of the information contained in the quantum system [15].

Furthermore, the "more conjugate" a measurement basis becomes relative to the state which has been used for preparing this quantum, the "more unpredictable" and thus "more indeterminate" in statistical terms the quantum behaves. In particular, if the state prepared is orthogonal to the projection observable measured (i.e. if there is a "maximal mismatch" between preparation and measurement), then the individual quantum not only cannot be predicted with certainty by any agent, but such an agent can do no better than blindly guessing the outcome of the measurement.

This, however, should not be understood as a claim that quantum randomness is "maximally random". Indeed, randomness can come in many flavours, from statistical properties to computability theoretic properties of outcome sequences. Maximal randomness in the sense that no correlations exist between successive measurement results is in fact mathematically impossible [16, 17]: there exist only degrees of randomness to which there is no upper limit. Thus, while there is a clear intuitive link between unpredictability and randomness of any kind, the link between indeterminism and unpredictability seems stronger than that with randomness, and any claims of quantum randomness need to be analysed carefully from a theoretical viewpoint. We will return to this point later in the paper.

III. MODELLING PREDICTION

A. Discussion of models of prediction

Various definitions of predictability have been proposed by different authors. While some authors, particularly in physics and cryptographic fields seem to adopt the view that probability mean unpredictability [4, 18], this is insufficient to describe unpredictable physical processes. Probabilities are a formal description given by a particular theory, but do not entail that a physical process is fundamentally indeterministic nor unpredictable, and can (often very reasonably) represent simply a lack of knowledge or underdetermination of the theory. Instead, a more robust way to formulate prediction seems to be in terms of a 'predicting agent' of some form. This appears to be what EPR had in mind when alluding to prediction in the EPR principle, and is similarly the approach taken by other more serious definitions to define predictability.

In the theory of dynamical systems, unpredictability has long been linked to chaos, and has often been identified as the inability to calculate with any reasonable precision the state of system given a particular observable initial condition [19]. The observability is critical, since although a system may presumably have a well-defined initial state (a point in phase-space), any observation yields an interval of positive measure (a region of phase space.) This certainly seems the correct path to follow in formalising predictability, but more generality and formalism is needed to provide a definition for arbitrary physical processes.

Popper, in arguing that unpredictability *is* indeterminism, defines prediction in terms of "physical predicting machines" [20]. He consider these as real machines that can take measurements of the world around them, compute via physical means, and output (via some display or tape, for example) predictions of the future state of the system. He then considers various prediction tasks, which can be thought of as experiments which must be predicted to a certain accuracy, and considers these to be predictable if it is *physically* possible to construct a predictor for them.

A more modern and technical definition was given by Eagle [21] in defining randomness as maximal unpredictability. While we will return to the issue of randomness later, his definition of unpredictability deserves further attention. He defined prediction relative to a particular theory, and for a particular predicting agent. Specifically, a prediction function is defined as a function mapping the state of the system described by the theory and specified epistemically (and thus finitely) by the agent to a probability distribution of states at some time t. This definition formalises more clearly prediction as the output of a function operating on information extracted about the physical system by an agent.

Here we wish to propose a definition of prediction that, while similar in many aspects to these definitions, addresses what we consider some conceptual and formal concerns with these formalisms. Popper's definition is perhaps not abstract enough and lacks generality by requiring the predictor to be physically present in its environment. Similarly, Eagle's definition renders predictability relative to a particular physical theory. In order to relate the intrinsic indeterminism of a system to unpredictability, it would be more appropriate to have a definition of events as unpredictable *in principle*. Thus, being ignorant of a better theory might change our epistemic ability to know if an event is predictable or not, but would not change the fact that an event may or may not be, in principle, predictable. Furthermore, we think it is important to restrict the class of prediction functions by imposing some effectivity (i.e. computability) constraints. Indeed, to predict is to say in advance via some effective means. It seems difficult to envisage a predicting agent operating by any other means, and giving the agent more power can further lead to technical difficulties by using incomputable numbers to 'cheat' in prediction.

Here we propose a definition that takes these points into account, giving a definition based on the ability for some computably operating agent to predict using finite information extracted from the system for a specified experiment. For simplicity we will consider tasks with binary observable values (0 or 1), but the extension to finitely or countable many (i.e. finitely specified) output values is trivial. Further, unlike Eagle [21] we consider only prediction with certainty, rather than with probability.While it is not difficult or too unreasonable to extend this to the more general scenario, this is not needed to discuss indeterminism, as the EPR principle indicates, and in doing so we avoid any potential pitfalls with probably 1 or 0 events [22].

While it is important to discuss the unpredictability of individual events [21], an issue that needs to be considered is when to consider such predictions correct, as we need to exclude the possibility that such a correct prediction can occur by chance.

Popper succinctly summarises this predicament in Ref. [20, 117–118]: "*If we assert of an observable event that it is unpredictable we do not mean, of course, that it is logically or physically impossible for anybody to give a correct description of the event in question before it has occurred; for it is clearly not impossible that somebody may hit upon such a description accidentally. What* *is asserted is that certain rational methods of prediction break down in certain cases—the methods of prediction which are practised in physical science.*"

One possibility is then to demand a proof that the prediction will be correct—to formalise the "rational methods of prediction" that Popper refers to. However, this is notoriously difficult and must be made relative to the physical theory considered, which generally is not well axiomatised. Instead we demand that such predictions be *repeatable*, and not merely one-off events. This point of view is consistent with Popper's own framework of empirical falsification [23, 24]: an empirical theory (in our case, the prediction) can never be proven correct, but it can be falsified through decisive experiments (an incorrect prediction). Specifically, we require that in any potential infinite set of repetitions the predictions remain correct.

B. Developing the model

In order to formalise our non-probabilistic model of prediction we considering a hypothetical experiment E specified effectively by an experimenter. We formalise the notion of a predictor, which is an effective (i.e. computational) method of uniformly predicting the outcome of an experiment using information extracted (again, uniformly) from the experimental conditions and the specification of the experiment. An experiment will be predictable if any potential sequence of repetitions (of unbounded length) of it can always be predicted correctly by such a predictor.

More formally, we consider a physical experiment E producing a single bit $x \in \{0,1\}$. An example of such an experiment is the measurement of a photon's polarisation after it has passed through a 50-50 beam splitter. As it will be seen later, the proposed framework can apply equally to other experiments. Further, with a particular instantiation or "trial" of E we associate the parameter λ, encoded as a real number, which fully describes the trial. While λ is not in its entirety an obtainable quantity, it contains any information that may be pertinent to prediction and we may have practical access to finite aspects of this information. In particular this information may be directly associated with the particular trial of E (e.g. initial conditions or hidden variables) and/or relevant external factors (e.g. the time, results of previous trials of E). Any such external factors should, however, be local in the sense of special relativity, as (even if we admit quantum nonlocality) any other information cannot be utilised for the purpose of prediction [10]. We can view λ as resource that one can extract finite information from in order to predict the outcome of the experiment E. We formalise this in the following.

An *extractor* is a function selecting a “finite” amount of information included in λ which can be used to make predictions of experiments performed with parameter λ. Formally, an extractor is a (deterministic) function $\lambda \mapsto \langle\lambda\rangle$ mapping reals to rationals. For example, $\langle\lambda\rangle$ may be an encoding of the result of the previous instantiation of E, or the time of day the experiment is performed.

A predictor for E is an algorithm (computable function) P_E which *halts* on every input and *outputs* either 0, 1 (cases in which P_E has made a prediction), or “prediction withheld”. We interpret the last form of output as a refrain from making a prediction. The predictor P_E can utilise as input the information $\langle\lambda\rangle$ selected by an extractor encoding relevant information for a particular instantiation of E, but, *as required by* EPR, must not disturb or interact with E in any way; that is, it must be *passive*.

As we noted earlier, a certain predictor may give the correct output for a trial of E simply by chance. This may be due not only to a lucky choice of predictor, but also to the input being chosen by chance to produce the correct output. Thus, we rather consider the performance of a predictor P_E using, as input, information extracted by a particular fixed extractor. This way we ensure that P_E utilises in ernest information extracted from λ, and we avoid the complication of deciding under what input we should consider P_E’s correctness.

A predictor P_E provides a *correct prediction* using the extractor $\langle\,\rangle$ for an instantiation of E with parameter λ if, when taking as input $\langle\lambda\rangle$, it outputs 0 or 1 (i.e. it does not refrain from making a prediction) and this output is equal to x, the result of the experiment.

Let us fix an extractor $\langle\,\rangle$. The predictor P_E is $k,\langle\,\rangle$*-correct* if there exists an $n \geq k$ such that when E is repeated n times with associated parameters $\lambda_1,\ldots,\lambda_n$ producing the outputs $x_1,x_2,\ldots,x_n$, P_E outputs the sequence $P_E(\langle\lambda_1\rangle),P_E(\langle\lambda_2\rangle),\ldots,P_E(\langle\lambda_n\rangle)$ with the following two properties: (i) no prediction in the sequence is incorrect, and (ii) in the sequence there are k correct predictions. The trials of E form a succession of events of the form “E is prepared, performed, the result recorded, E is reset”, iterated n times in an algorithmic fashion.

If P_E is $k,\langle\,\rangle$-correct we can bound the probability that P_E is in fact operating by chance and may not continue to give correct predictions, and thus give a measure of our confidence in the predictions of P_E. Specifically, the sequence of n predictions made by P_E can be represented as a string of length n over the alphabet $\{T,F,W\}$, where T represents a correct prediction, F an incorrect prediction, and W a withheld prediction. Then, for a $k,\langle\,\rangle$-correct predictor there exists an $n \geq k$ such that the sequence of predictions contains k T’s and $(n-k)$ W’s. There are $\binom{n}{k}$ such possible prediction sequences out of 3^n possible strings of length n. Thus, the probability that such a correct sequence would be produced by chance is

$$\frac{\binom{n}{k}}{3^n} < \frac{2^n}{3^n} \leq \left(\frac{2}{3}\right)^k.$$

Clearly the confidence we have in a $k, \langle\,\rangle$-correct predictor increases as $k \to \infty$. If P_E is $k, \langle\,\rangle$-correct for all k, then P_E never makes an incorrect prediction and the number of correct predictions can be made arbitrarily large by repeating E enough times.

The definition of $k, \langle\,\rangle$-correctness allows P_E to refrain from predicting when it is unable to. A predictor P_E which is $k, \langle\,\rangle$-correct for all k, is, when using the extracted information $\langle\lambda\rangle$, guaranteed to always be capable of providing more correct predictions for E, so it will not output "prediction withheld" indefinitely. Furthermore, although P_E is technically used only a finite, but arbitrarily large, number of times, the definition guarantees that, in the hypothetical scenario where it is executed infinitely many times, P_E will provide infinitely many correct predictions and not a single incorrect one.

While a predictor's correctness is based on its performance in repeated trials, we can use the predictor to define the prediction of single bits produced by the experiment E. If P_E is not $k, \langle\,\rangle$-correct for all k, then we cannot exclude the possibility that any correct prediction P_E makes is simply due to chance. Hence, we propose the following definition: *the outcome x of a single trial of the experiment E performed with parameter λ is* predictable *(with certainty) if there exist an extractor $\langle\,\rangle$ and a predictor P_E which is $k, \langle\,\rangle$-correct for all k, and $P_E(\langle\lambda\rangle) = x$.*

IV. MAXIMAL INCOMPUTABILITY

The formal and physically motivated model of prediction we have presented can be applied to any physical experiment. However, let us turn our attention to using it to categorise more rigorously the unpredictability of quantum measurement outcomes discussed in Sec. II C.

We first show that experiments utilising quantum value indefinite observers cannot have a predictor which is $k, \langle\,\rangle$-correct for all k. More precisely: *if E is an experiment measuring a quantum value indefinite observer, then for every predictor P_E using any extractor $\langle\,\rangle$, P_E is not $k, \langle\,\rangle$-correct for all k.*

Throughout this section we will consider an experiment E performed in dimension $n \geq 3$ Hilbert space in which a quantum system is prepared in a state $|\psi\rangle$ and a value indefinite observable P_ϕ is measured producing a single bit x. By Theorem 1 such an observable is guaranteed to exist, and to identify one we need only a mismatch between preparation and observation contexts. The nature of the physical system in which this state is prepared and the experiment performed is not important, whether it be photons passing through generalised beam splitters [25], ions in an atomic trap, or any other quantum system in dimension $n \geq 3$ Hilbert space.

Let us fix an extractor $\langle\,\rangle$, and assume for the sake of contradiction that there exists a predictor P_E for E which is $k, \langle\,\rangle$-correct for all k. Consider the hypothetical situation where the experiment E is repeatedly initialised, performed and reset *ad infinitum* in an algorithmic "ritual" generating an infinite sequence of bits $\mathbf{x} = x_1 x_2 \dots$

Since P_E *never* makes an incorrect prediction, each of its predictions is correct with certainty. Then, according to the EPR principle we must conclude that each such prediction corresponds to a value definite property of the system measured in E. However, we chose E such that this is not the case: each x_i is the result of the measurement of a value indefinite observable, and thus we obtain a contradiction and conclude no such predictor P_E can exist.

Moreover, since there does not exist a predictor P_E which is $k, \langle\,\rangle$-correct using any extractor $\langle\,\rangle$ for all k, for such a quantum experiment E, no single outcome is predictable with certainty. Stated differently, in an infinite repetition of E as considered previously generating the infinite sequence $\mathbf{x} = x_1 x_2 \dots$, *no single bit x_i can be predicted with certainty.*

A further consequence of this result is that the sequence $\mathbf{x}$ must be strongly incomputable, technically *bi-immune*.[26] This was shown in [8, 27], but follows directly and more naturally from this new formalism of prediction.

Let us assume for the sake of contradiction that $\mathbf{x} = x_1 x_2 \dots$ is not bi-immune. Then, from the definition of bi-immunity, there exist an infinite computable set $I \subset \mathbb{N}^+$ and a partially computable function f whose domain is I and satisfies $f(i) = x_i$ for every $i \in I$. Consider the extractor $\langle \lambda_i \rangle = i$. Now we can use f to construct a predictor P_E which is $k, \langle\,\rangle$-correct for all $k > 0$. On the ith iteration of E with parameter λ_i,

$$P_E(\langle \lambda_i \rangle) = \begin{cases} f(i) = x_i, & \text{if } i \in I, \\ \text{"prediction withheld"}, & \text{if } i \notin I. \end{cases}$$

It is clear by the properties of f that P_E indeed satisfies the criteria to be $k, \langle\,\rangle$-correct for all k: each bit $x_{f(i)}$ for $i \in I$, for which there are infinitely many, is correctly predicted. Thus, since no such predictor can exist, the sequence $\mathbf{x}$ must be bi-immune; in particular, $\mathbf{x}$ is *incomputable*.

V. SUMMARY

The main thrust of our argument has been to formally certify the indeterminism of single quantum events and their consequential unpredictability, rather than rely on the *ad hoc* postulation of these properties. In particular, suppose that we prepare a quantum in a pure state corresponding to a unit vector in Hilbert space of dimension at least three. Then any complementary observable property of this quantum—corresponding to some projector whose respective linear subspace is neither collinear nor orthogonal with respect to the pure state vector—has no predetermined value, and thus remains value indefinite. Furthermore, we show that the outcome of a measurement of such a property is unpredictable with respect to a very general model of prediction. These results are true relative to the assumptions made, in particular, admissibility, noncontextuality, and the eigenstate principle.

In other terms the bit resulting from the measurement of such an observable property is "created from nowhere", and cannot be causally connected to any physical entity, whether it be knowable in practice or hidden. One might say that the quantum system acts like an *incomputable oracle.*

This irreducible indeterminacy "certifies" the use of quantum random number generators for various computational tasks in cryptography and elsewhere [28–30]. Our results can also be interpreted as justification for certain claims of *hypercomputation*, as no universal Turing machine will ever be able to produce in the limit an output that is identical with the sequence of bits generated by a quantum oracle [31]. More than that—no single bit of such sequences can ever be predicted.

As a concluding remark, we emphasise that the indeterminism and unpredictability of quantum measurement outcomes are based on the results of strong forms of the Kochen-Specker theorem, and hence require at minimum three-dimensional Hilbert space. This requirement is necessary to ensure the nontrivial interconnectedness of contexts (i.e. maximal sets of compatible observables) used to derive such results. We thus strongly recommend the use of at least three-dimensional Hilbert space in the construction of quantum random number generators based on quantised systems and quantum indeterminism.

ACKNOWLEDGEMENT

This work was supported in part by Marie Curie FP7-PEOPLE-2010-IRSES Grant RANPHYS.

[1] Wayne C. Myrvold, "Statistical mechanics and thermodynamics: A Maxwellian view," Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics **42**, 237–24

[2] Max Born, "Zur Quantenmechanik der Stoßvorgänge," Zeitschrift für Physik **37**, 863–867 (1926).

[3] Max Born, *Physics in my generation*, 2nd ed. (Springer, New York, 1969).

[4] Anton Zeilinger, "The message of the quantum," Nature **438**, 743 (2005).

[5] John S. Bell, "On the problem of hidden variables in quantum mechanics," Reviews of Modern Physics **38**, 447–452 (1966).

[6] Simon Kochen and Ernst P. Specker, "The problem of hidden variables in quantum mechanics," Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal) **17**, 59–87 (1967).

[7] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger, "Violation of Bell's inequality under strict Einstein locality conditions," Physical Review Letters **81**, 5039–5043 (1998).

[8] Alastair A. Abbott, Cristian S. Calude, Jonathan Conder, and Karl Svozil, "Strong Kochen-Specker theorem and incomputability of quantum randomness," Physical Review A **86**, 062109 (2012), arXiv:1207.2029.

[9] Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

[10] Franck Laloë, *Do We Really Understand Quantum Mechanics?* (Cambridge University Press, Cambridge, 2012).

[11] Mauricio Suárez, "Quantum Selections, Propensities and the Problem of Measurement," The British Journal for the Philosophy of Science **55**, 219–255 (2004).

[12] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, "Value-indefinite observables are almost everywhere," Physical Review A **89**, 032109 (2014), arXiv:1309.7188.

[13] David Bohm, "A suggested interpretation of the quantum theory in terms of "hidden" variables. I,II," Physical Review **85**, 166–193 (1952).

[14] John S. Bell, "Against 'measurement'," Physics World **3**, 33–41 (1990).

[15] T. Paterek, J. Kofler, R. Prevedel, P. Klimek, M. Aspelmeyer, A. Zeilinger, and Č Brukner, "Logical independence and quantum randomness," New Journal of Physics **12**, 013019 (2010).

[16] Ronald Graham and Joel H. Spencer, "Ramsey theory," Scientific American **262**, 112–117 (1990).

[17] Cristian Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).

[18] Antonio Acín, "True quantum randomness," in *Is Science Compatible with Free Will?: Exploring Free Will and Consciousness in the Light of Quantum Physics and Neuroscience*, edited by A. Suarez and P. Adams (Springer, 2013) Chap. 2, pp. 7–22.

[19] Charlotte Werndl, "What are the new implications of chaos for unpredictability?" British Journal for the Philosophy of Science **60**, 195–220 (2009).

[20] Karl Raimund Popper, "Indeterminism in quantum physics and in classical physics I," The British Journal for the Philosophy of Science **1**, 117–133 (1950).

[21] Antony Eagle, "Randomness is unpredictability," British Journal for the Philosophy of Science **56**, 749–790 (2005).

[22] Asad Zaman, "On the impossibility of events of zero probability," Theory and Decision **23**, 157–159 (1987).

[23] Karl Raimund Popper, *Logik der Forschung* (Springer, Vienna, 1934).

[24] Karl Raimund Popper, *The Logic of Scientific Discovery* (Basic Books, New York, 1959).

[25] M. Reck, Anton Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," Physical Review Letters **73**, 58–61 (1994).

[26] A bi-immune sequence is one that contains no infinite computable subsequence.

[27] Cristian S. Calude and Karl Svozil, "Quantum randomness and value indefiniteness," Advanced Science Letters **1**, 165–168 (2008), eprint arXiv:quant-ph/0611029, arXiv:quant-ph/0611029.

[28] Karl Svozil, "The quantum coin toss—testing microphysical undecidability," Physics Letters A **143**, 433–437 (1990).

[29] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical quantum random number generator," Journal of Modern Optics **47**, 595–598 (2000).

[30] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[31] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, “A quantum random oracle,” in *Alan Turing: His Work and Impact*, edited by S. Barry Cooper and J. van Leeuwen (Elsevier Science, 2013) pp. 206–209.