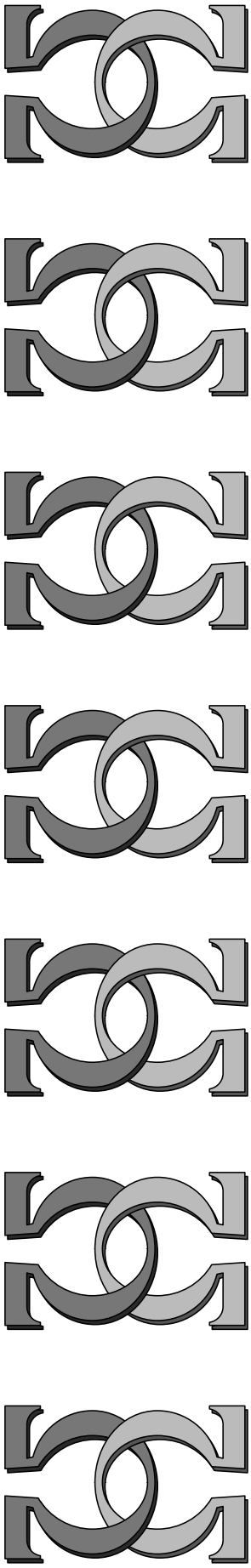

CDMTCS
Research
Report
Series

On the Unpredictability of Individual Quantum Measurement Outcomes

A. A. Abbott[1,2], C. S. Calude[1], K. Svozil[1,3]

[1]University of Auckland, NZ
[2]ENS, Paris, France
[3]Vienna University of Technology, Austria

CDMTCS-458
March 2014

Centre for Discrete Mathematics and
Theoretical Computer Science

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: August 14, 2014)

Abstract

We develop a general, non-probabilistic model of prediction which is suitable for assessing the (un)predictability of individual physical events. We use this model to provide, for the first time, a rigorous proof of the unpredictability of a class of individual quantum measurement outcomes, a well-known quantum attribute postulated or claimed for a long time.

We prove that quantum indeterminism—formally modelled as value indefiniteness—-is incompatible with the supposition of predictability: value indefinite observables are unpredictable. The proof makes essential use of a strengthened form of the Kochen-Specker theorem proven previously to identify value indefinite observables. As a result, quantum unpredictability, like the Kochen-Specker theorem, relies on three assumptions: compatibility with quantum mechanical predictions, non-contextuality, and the value definiteness of observables corresponding to the preparation basis of a quantum state.

Finally, quantum unpredictability is used to prove that quantum randomness is "maximally incomputable" and to discuss a real model of hypercomputation whose computational power has yet to be determined. The paper ends with a further open problem.

* 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

The outcomes of measurements on a quantum systems are often regarded to be fundamentally unpredictable [1]. However, such claims are based on intuition and experimental evidence, rather than precise mathematical reasoning. In order to investigate this view more precisely, both the notion of unpredictability and the status of quantum measurements relative to such a notion need to be carefully studied.

Unpredictability is difficult to formalise not just in the setting of quantum mechanics, but that of classical mechanics too. Various physical processes from classical chaotic systems to quantum measurement outcomes are often considered unpredictable, and various definitions, both domain specific [2] and more general [3], and of varying formality, have been proposed. For precise claims to be made, the appropriate definitions need to be scrutinised and the results proven relative to specific definitions.

Quantum indeterminism has been progressively formalised via the notion of value indefiniteness in the development of the theorems of Bell [4] and, particularly, Kochen and Specker [5]. These theorems, which have also been experimentally tested via the violation of various inequalities [6], express the impossibility of certain classes of deterministic theories. The conclusion of value indefiniteness from these no-go theorems rests on various assumptions, amounting to the refusal to accept non-classical alternatives such as non-locality and contextual determinism. And if value indefiniteness is, as often claimed, related to unpredictability, any claims of unpredictability need to be similarly evaluated with respect to, and seen to be contingent on such assumptions.

In this paper we address these issues in turn. We first discuss various existing notions of predictability and their applicability to physical events. We propose a new formal model of prediction which is non-probabilistic and, we argue, captures the notion that an arbitrary single physical event (be it classical, quantum, or otherwise) or sequence thereof is 'in principle' predictable. We review the formalism of value indefiniteness and the assumptions of the Kochen-Specker theorems (classical and stronger forms), and show that the outcomes of measurements of value indefinite properties are indeed unpredictable with respect to our model. Thus, in this framework unpredictability rests on the same assumptions as quantum value indefiniteness. Finally, we discuss the relationship between quantum randomness and unpredictability, and show that unpredictability implies the strong incomputability of sequences of quantum measurement outcomes.

II. MODELS OF PREDICTION

Various definitions of predictability proposed by different authors will be discussed regarding their suitability for capturing the notion of predictability of individual physical events or sequences thereof in the most general sense. While some authors, particularly in physics and cryptographic fields, seem to adopt the view that probabilities mean unpredictability [1, 7], 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, that is, ontologically, indeterministic nor unpredictable, and can (often very reasonably) represent simply an epistemic 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 is indeed the approach taken by some definitions, and that we also will follow.

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 a system given a particular observable initial condition [2]. 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" [8]. He considers 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 studies experiments which must be predicted with 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 [3] in defining randomness as maximal unpredictability. While we will return to the issue of randomness later, Eagle's 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. This definition formalises more clearly prediction as the output of a function operating on information extracted about the

physical system by an agent.

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. Furthermore, 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, the predictor's ignorance of a better theory might change their associated 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. Last but not least, 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 in an effective/constructive/computable way (e.g. by calculating with an algorithm). Any predicting agent operating with incomputable means—incomputable/infinite inputs or procedures that can go beyond the the power of algorithms (for example, by executing infinitely many operations in a finite amount of time)—seems to be physically highly speculative if not impossible. Technically, "controlled incomputability" could be easily incorporated in the model, if necessary.

Taking these points into account, we propose a definition—similar in many aspects to Popper's and Eagle's definitions—based on the ability of some computably operating agent to correctly predict using finite information extracted from the system of the 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 straightforward. Further, unlike Eagle [3], we consider only prediction with certainty, rather than with probability. While it is not difficult nor unreasonable to extend our definition to the more general scenario, this is not needed for our application to quantum measurements; moreover, in doing so we avoid any potential pitfalls related to probability 1 or 0 events [9].

Our main aim is to define the (correct) prediction of individual events [3], which can be easily extended to an infinite sequence of events. An individual event can be correctly predicted simply by chance, and a robust definition of predictability clearly has to avoid this possibility. Popper succinctly summarises this predicament in Ref. [8, 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 is correct, thus formalising 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 and can change over time. 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 [10, 11]: an empirical theory (in our case, the prediction) can never be proven correct, but it can be falsified through decisive experiments pointing to incorrect predictions. Specifically, we require that the *predictions remain correct in any arbitrarily long (but finite) set of repetitions of the experiment.*

III. A MODEL FOR PREDICTION OF INDIVIDUAL PHYSICAL EVENTS

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

In detail, we consider a finitely specified physical experiment E producing a single bit $x \in \{0,1\}$ (which, as we previously noted, can readily be generalised). Such an experiment could, for example, be the measurement of a photon's polarisation after it has passed through a 50-50 polarising beam splitter, or simply the toss of a physical coin with initial conditions and experimental parameters specified finitely. 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 any predictor can have practical access to a finite amount 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 non-locality) any other information cannot be utilised for the purpose of prediction [12].

We can view λ as a 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 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:

1. no prediction in the sequence is incorrect, and

2. 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 tends to zero when k goes to infinity because

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

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 $P_E(\langle\lambda\rangle) = x$.*

Accordingly, P_E correctly predicts the outcome x, never makes any incorrect prediction, and can produce arbitrarily many correct predictions.

IV. QUANTUM UNPREDICTABILITY

We now wish to apply the above definition to formally justify the well-known claim that quantum events are completely unpredictable.

A. The intuition of quantum indeterminism and unpredictability

Intuitively, it would seem that quantum indeterminism 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 indeterminate. That is, for such an observable none of the possible exclusive measurement outcomes are 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. For example, an agent trying to predict the outcome of a measurement of a projection observable orthogonal to the state prepared (i.e. if there is a "maximal mismatch" between preparation and measurement) could do no better than blindly guess the outcome of the measurement. preparation and measurement) could do no better than blindly guess the outcome of the measurement.

However, such an argument is too informal. To apply our model of unpredictability the notion of indeterminism needs to be specified much more rigorously: this implies developing a formalism for quantum indeterminism, as well as a careful discussion of the assumptions which indeterminism is reliant on.

B. A formal basis for quantum indeterminism

The 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. 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 [13], expresses fundamental, irreducible indeterminism [14]. 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 [15, p. 204] "*He does not throw dice*." Nonetheless, over time the conjecture that measurement outcomes are themselves fundamentally indeterministic became the quantum orthodoxy [1].

Beyond the blind belief originating with Born, the Kochen-Specker theorem, along with Bell's theorem, are among the primary reasons for the general acceptance of quantum indeterminism.

The belief in quantum indeterminism thus rests largely on the same assumptions as these theorems. In the development of the Kochen-Specker theorem, quantum indeterminism has been formalised as the notion of value indefiniteness [16], which allows us to discuss indeterminism in a more general formal setting rather than restricting ourselves to any particular interpretation. Here we will review this formalism, as well as a stronger form of the Kochen-Specker theorem and its assumptions which are important for the discussion of unpredictability.

For a given quantum system in a particular state, we say that an observable is *value definite* if the measurement of that observable is pre-determined to take a (potentially hidden) value. If no such pre-determined value exists, the observable is *value indefinite*. Formally, this notion can be represented by a *(partial) value assignment function* (see [16] for the complete formalism).

In addressing the question of 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 [17, p. 777]. Based on this accepted notion of an element of physical reality, we allow ourselves to be guided by the following "EPR principle", 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 non-trivial [12], but is equally required by our model of prediction.

The EPR principle justifies the subtle but often overlooked

> *Eigenstate principle*: 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 principle is necessary in order to use the strong Kochen-Specker theorem to single-out value indefinite observables, and is similar to, although weaker, than the eigenstate-eigenvalue link (as only one direction of the implication is asserted) [18].

A further requirement called *admissibility* is used to avoid outcomes impossible to obtain according to quantum predictions. Formally, admissibility states that an observable in a context—i.e. a set of mutually commuting (i.e. compatible) observables—cannot be value indefinite if all but one of the possible measurement outcomes would contradict quantum mechanical identities given

the values of other, value definite observables in the same context. In such a case, the observable must have the definite value of that sole 'consistent' measurement outcome.

Here is an example: given a context $\{P_1, \ldots, P_n\}$ of commuting projection observables, if P_1 were to have the definite value 1, all other observables in this context 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 prediction that one and only one projector in a context give the value 1 on measurement. Note that we require this to hold only when any indeterminism (which implies multiple possible outcomes) would allow quantum mechanical predictions to be broken: were P_1 to have the value 0, admissibility would not require anything of the other observables if the rest were value indefinite, as neither a measurement outcome of 0 or 1 for $P_2 \ldots P_n$ would lead to a contradiction.

The Kochen-Specker theorem [5] 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 go deeper and localise value indefiniteness to prove 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-contextually, without requiring that all observables be value definite. Thus, any mismatch between preparation and measurement context leads to the measurement of a value indefinite observable: this is stated formally in the following strong version of the Kochen-Specker theorem.

Theorem 1 (From [16, 19])**.** *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 value assignment.*

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.

C. Contextual alternatives

It is worth keeping in mind that, while indeterminism is often treated as an assumption or aspect of the orthodox viewpoint [1, 14], this usually rests implicitly on the deeper assumptions

(mentioned in Section IV B) that the Kochen-Specker theorem relies on. If these assumptions are violated, deterministic theories could not be excluded, and the status of value indefiniteness and unpredictability would need to be carefully revisited.

If this were the case, perhaps the simplest alternative would be the explicit assumption of (albeit non-local) context dependant predetermined values. Many attempts to interpret quantum mechanics deterministically, such as Bohmian mechanics [20], can be expressed in this framework. Since such a theory would no longer be indeterministic, the intuitive argument for unpredictability would break down, and the theory could in fact be totally predictable. 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).

Another possibility would be to consider the case that any predetermined outcomes may in fact not be determined by the observable alone, but rather by *"the complete disposition of the apparatus"* [4, Sec. 5]. 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 unpredictability* 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 case, just as for irreversibility in classical statistical mechanics [13], the unpredictability 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.

D. Unpredictability of individual quantum measurements

With the notion of value indefiniteness presented, let us now turn our attention to applying our formalism of unpredictability to quantum measurement outcomes of the type discussed in Section IV B.

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 [21], ions in an atomic trap, or any other quantum system in dimension $n \geq 3$ Hilbert space.

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:

Theorem 2. *If E is an experiment measuring a quantum value indefinite observervable, then for every predictor P_E using any extractor $\langle\rangle$, P_E is not $k, \langle\rangle$-correct for all k.*

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 $\mathbf{x} = x_1 x_2 \ldots$

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.

Theorem 3. *In an infinite repetition of E generating the infinite sequence $\mathbf{x} = x_1 x_2 \ldots$ as described above, no single bit x_i can be predicted with certainty.*

V. MAXIMAL INCOMPUTABILITY AND QUANTUM RANDOMNESS

While there is a clear intuitive link between unpredictability and randomness, it is an important point that the unpredictability of quantum measurement outcomes should not be understood to mean that that quantum randomness is "truly random". Indeed, the subject of randomness is a delicate one: randomness can come in many flavours [22], from statistical properties to computability

theoretic properties of outcome sequences. For physical systems, the randomness of a process also needs to be differentiated from that of its outcome.

As mentioned earlier, Eagle has argued that a physical process is random if it is "maximally unpredictable" [3]. In this light it may be reasonable to consider quantum measurements as random events, giving a more formal meaning to the notion of "quantum randomness". However, given the intricacies of randomness, it should be clear that this refers to the measurement *process*, and does not entail that quantum measurement outcomes are maximally random. In fact, maximal randomness in the sense that no correlations exist between successive measurement results is mathematically impossible [23, 24]: there exist only degrees of randomness with no upper limit. As a result, any claims regarding the quality of quantum randomness need to be analysed carefully.

Indeed, in many applications of quantum randomness stronger computability theoretic notions of randomness, such as Martin-Löf randomness [24], which apply to sequences of outcomes would be desirable. *It is not known if quantum outcomes are indeed random in this respect.* However, it is true that a sequence $\mathbf{x}$ produced by repeated outcomes must be strongly incomputable, technically *bi-immune*. A sequence is bi-immune if it contains no infinite computable subsequence; this property, which is weaker than algorithmic (Martin-Löf) randomness, is a minimal symptom of a robust form of randomness. The above result was shown in [16, 25], but follows directly and more naturally from the new formalism of prediction.

For the sake of a proof by contradiction let us assume that $\mathbf{x} = x_1 x_2 \ldots$ 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*.

Incomputability appears *maximally* in two forms: *individualised*—no single bit can be predicted with certainty (Theorem 3), i.e. an algorithmic computation of a single bit, even if correct, cannot be formally certified; and *asymptotic* via bi-immunity—only finitely many bits can be cor-

rectly predicted via an algorithmic computation.

VI. SUMMARY

In this paper, we addressed two specific points relating to physical unpredictability. Firstly, we developed a generalised model of prediction for both individual physical events, and (by extension) infinite repetitions thereof. This model formalises the notion of an effective prediction agent being able to predict 'in principle' the outcome of an effectively specified physical experiment. This model can be applied to classical or quantum systems of any kind to assess their (un)predictability, and doing so to various systems, particularly classical, could be an interesting direction of research for the future.

Secondly, we applied this model to quantum measurement events. Our goal was to formally deduce the unpredictability of single quantum measurement events, via the strong Kochen-Specker theorem and value indefiniteness, rather than rely on the *ad hoc* postulation of these properties.

More specifically, 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—is value indefinite. Furthermore, the outcome of a measurement of such a property is unpredictable with respect to our model of prediction.

Quantum value indefiniteness is key for the proof of unpredictability. In this framework, the bit resulting from the measurement of such an observable property is "created from nowhere" (*creatio ex nihilo*), 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.* While quantum indeterminism is often informally treated as an assumption in and of itself, it is better seen as a formal consequence of Kochen-Specker theorems in the form of value indefiniteness. (Indeed, without these theorems such an assumption would appear weakly grounded.) Yet this derivation of value indefiniteness rests on the three assumptions: admissibility, non-contextuality, and the eigenstate principle. As we discussed in Section IV C, models in which some of these assumptions are not satisfied exist.

The unpredictability of quantum measurements "certifies" the use of quantum random number generators for various computational tasks in cryptography and elsewhere [26–28]. Our results

can also be interpreted as a justification for a form 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 [29]. More than that—no single bit of such sequences can ever be predicted. Evaluating the computational power of a (universal) Turing machine provided with a quantum random oracle certified by maximum unpredictability is a challenging, both theoretical and practical, *open problem*.

Finally, we emphasise that the indeterminism and unpredictability of quantum measurement outcomes proved in this paper are based on the strong form of the Kochen-Specker theorem, and hence require at minimum three-dimensional Hilbert space. The question of whether this result can also proven for two-dimensional Hilbert space without simply assuming value indefiniteness is an *open problem*; this question is important not only theoretically, but also practically, because many current quantum random generators are based on two-dimensional measurements.

ACKNOWLEDGEMENT

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

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

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

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

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

[5] 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).

[6] 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).

[7] 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.

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

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

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

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

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

[13] 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**, 237–243 (2011).

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

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

[16] 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.

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

[18] Mauricio Suárez, "Quantum selections, propensities and the problem of measurement," The British Journal for the Philosophy of Science **55**, 219–255 (2004).

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

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

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

[22] R. Downey and D. Hirschfeldt, *Algorithmic Randomness and Complexity* (Springer, Berlin, 2010).

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

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

[25] 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.

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

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

[28] 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).

[29] 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.