CDMTCS Research Report Series

Complementarity and the (Un)Predictability of 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-477
February 2015

Centre for Discrete Mathematics and
Theoretical Computer Science

Complementarity and the (Un)Predictability of 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, République des Savoirs, USR 3608, CNRS,*
Collège de France and 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: February 22, 2015)

In this paper we formally study the unpredictability of measurements of complementary observables, in quantum and classical mechanics. To do so, we extend a formal model of unpredictability we previously developed to allow for more nuanced, relativised notions of unpredictability, as needed for this purpose. This model of relativised unpredictability is, for instance, also well suited to the study of finite-time unpredictability in chaotic systems.

We use this model to show that complementarity implies only a form of relative unpredictable: measurements of complementary observables are unpredictable for an observer unable to measure properties of a system complementary to those known for the system. However, in contrast to measurements of quantum value indefinite observables, these measurement outcomes need not be absolutely unpredictable.

We further discuss the relationship between relative unpredictability and computability, and show that complementarity, again in contrast to value indefiniteness, does not guarantee incomputability—an algorithmic form of unpredictability: sequences generated by measurements of complementary observables can be computable.

Finally we discuss the use of complementarity in certifying quantum randomness, arguing that it is, by itself, a fairly weak property which is unable to provide the certification that quantum value indefiniteness, via the Kochen-Specker theorem, can.

* 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

It is generally thought that it is impossible to predict the value obtained upon measuring a quantum observable [1]. However, this view that quantum randomness is truly unpredictable (in contrast, for example, to pseudo-randomness) has often been expressed informally and the appropriate formal framework rigorous treatment has been lacking. Instead, many features of quantum mechanics have been loosely invoked to explain this: from the probabilities appearing in the Born rule, complementarity, to the Kochen-Specker theorem and Bell inequalities.

First and foremost, the notion of predictability itself is difficult to formalise, especially in the absolute sense (as opposed to the purely epistemic considerations present, for example, in probability theory) that the belief about quantum mechanics seems to require. In [2] we undertook to develop such a framework for predictability, and presented such a model than is suitable for discussing the ability to predict 'in principle' the result of arbitrary physical experiments and processes. We further used this framework to analyse quantum unpredictability, and we showed that value indefiniteness—a formalised notion of indeterminism arising from the Kochen-Specker theorem [3]—can be used to show that the outcomes of individual quantum outcomes are indeed absolutely unpredictable.

Unfortunately, the Kochen-Specker theorem only holds in a Hilbert space of dimension at least three, a formal restriction meaning the unpredictability of quantum measurements in two-dimensional spaces—such as for qubits—is less solidly grounded.

In this paper we look at another quantum phenomenon, complementarity, and its relation to unpredictability, in order to see if this can be used to deduce quantum unpredictability for systems of any dimension. To do so, we further develop the framework of unpredictability we introduced in [2], extending it to a relativised notion of unpredictability. That is, we allow one to consider the predictability of an experiment relative to the particular means/resources of a predicting agent. This allows us to consider more nuanced, epistemic notions of unpredictability and their relation to absolute unpredictability.

We then show that the measurements of quantum observables that are complementary to the observable used to prepare a state are unpredictable, not absolutely, but relative to a predicting agent whose measurement capabilities are limited by a complementarity principle, in a way which we will discuss rigorously. This relativisation is necessary due to the ability for complementarity to co-exist with value definiteness. Even if these limits are fundamental rather than epistemic (as perhaps many consider to be the case), we will discuss the fact that complementarity alone cannot guarantee this to be the case.

We discuss the relation between (relativised) unpredictability, complementarity and the computability of sequences produced by repeating quantum measurements *ad infinitum*. We show that, in contrast to value indefiniteness which leads to a strong form of incomputability, complementarity alone cannot exclude the computability of such a sequence, and thus perhaps should not be used alone to certify 'quantum randomness', as in many quantum random number generators [4]. We finish by summarising the relationship between the different notions of predictability, quantum value indefiniteness, complementarity, and computability.

II. PREDICTABILITY

In [2] we proposed a model of predictability based around the ability for an agent to, in principle, predict the outcome of a physical experiment. Here we refine this model to be able to relativise it with respect to the means/resources of the predicting agent: what is predictable to one agent may not be to another. This gives our model an epistemic element, where our previous and more objective model can be obtained as the limit case. In this framework we can consider the predictive capabilities of an agent with limited capacities imposed by practical limitations, or under the constraints of physical hypotheses restricting on such abilities.

While we refer the reader to [2] for a full motivation to our approach to modelling predictability, we note that the idea is to develop a notion of predictability for individual events by considering the ability for a predicting agent, acting via uniform, effective means, to predict correctly and reproducibly the outcome of an experiment using some finite information the agent extracts from the 'environment' as input. More precisely, the model consists of several elements:

1. The specification of an experiment E for which the outcome must be predicted.

2. A predicting agent or 'predictor', which must predict the outcome of the experiment. We model this as an effectively computable function, a choice which we will justify further.

3. An extractor ξ is a physical device the agent uses to (uniformly) extract information pertinent to prediction that may be outside the scope of the experimental specification E. This could be, for example, the time, measurement of some parameter, iteration of the experiment, etc.

4. A prediction made by the agent with access to a set Ξ of extractors.

We will next elaborate on the individual aspects of the model.

A. Predictability model

Experimental specification. An experiment is a finite specification for which the outcome is to be predicted. We restrict ourselves to the case where the result of the experiment, i.e. the value to be predicted, is a single bit: 0 or 1. However, this can readily be generalised for any finite outcome. On the other hand it does not make sense to predict an outcome requiring an infinite description, such as a real number, since this can never be measured exactly. In such a case the outcome would be an approximation of the real—a rational number, and thus finitely specifiable.

The experimental specification, being finite, can not normally specify exactly the required setup of the experiment, as a precise description of experimental conditions generally involves real-valued parameters. Rather, it is expressed with finite precision and with respect to the symmetries pertinent to the experimenter and their limited capacities. A particular trial of E is associated with the parameter λ which fully describes the "state of the universe" in which the trial is run. As an example, one could consider E to specify the flipping of a certain coin, or it could go further and specify, up to a certain accuracy, the initial dynamical conditions of the coin flip. In both cases, λ contains further details—such as the exact initial conditions—which could be used by an agent in trying to predict the result of E.

The parameter λ will generally[1] be "an infinite quantity"—for example, an infinite sequence or a real number—structured in an unknown manner. Forcing a specific encoding upon λ, such as a real number, may impose an inadequate structure (e.g. metric, topological) which is not needed for what follows. While λ is generally not in its entirety an obtainable quantity, it contains any information that may be pertinent to prediction—such as the time at which the experiment states, the precise initial state, any hidden parameters, etc.—and any predictor can have practical access to a finite amount of this information. We can view λ as a resource from which one can extract finite information in order to try and predict the outcome of the experiment E.

Predicting agent. The predicting agent (or 'predictor') is, as one might expect, the agent trying to predict the outcome of a particular experiment, using potentially some data obtained from the system (i.e. from λ) to help in the process. Since such an agent should be able to produce a prediction in a finite amount of time via some uniform procedure, we need the prediction to be *effective*.

Formally, we describe a predicting agent as a computable function P_E (i.e. an algorithm) which halts on every input and outputs either 0,1, or "prediction withheld". Thus, the agent may refrain from making a prediction in some cases if it is not certain of the outcome. P_E will generally be dependent on E, but its definition as an abstract algorithm means *it must be able to operate without interacting with the subsystem whose behaviour it predicts*.

We note finally that the choice of computability as the level of effectivity required can be strengthened or weakened, as long as some effectivity is kept. Our alternative choice here is motived by the Church-Turing thesis, a rather robust assumption [5].

Extractor. An extractor is a physically realisable device which a predicting agent can use to extract (finite) useful data that may not be a part of the description of E from λ to use for prediction—i.e. as input to P_E. In many cases this can be viewed as a measurement instrument, whether it be a ruler, a clock, or a more complicated device.

Formally, an extractor is a function $\lambda \mapsto \xi(\lambda) \in \{0,1\}^*$, where $\xi(\lambda)$ is a finite string of bits, which can be physically realised without altering the system, i.e. passively. In order to be used by P_E for prediction, $\xi(\lambda)$ should be finite and effectively codable, e.g. as a binary string or a rational number.

Prediction. We define now the notion of a correct prediction for a predicting agent having access to a fixed (finite or infinite) set Ξ of extractors.

Given a particular extractor ξ, we say the prediction of a run of E with parameter λ is *correct for* ξ if the output $P_E(\xi(\lambda))$ is the same as the outcome of the experiment. That is, it correctly predicts E when using information extracted from λ by ξ as input.

However, this is not enough to give us a robust definition of predictability, since for any given run it could be that we predict correctly by chance. To overcome this possibility, we need to consider the behaviour of repeated runs of predictions.

A *repetition procedure for E* is an algorithmic procedure for resetting and repeating the experiment E. Generally this will be of the form "E is prepared, performed and reset in a specific fashion". The specific procedure is of little importance, but the requirement is needed to ensure the way the experiment is repeated cannot give a predicting agent power that should be beyond their capabilities or introduce mathematical loopholes by 'encoding' the answer in the repetitions; both the prediction and repetition should be performed algorithmically.

We say the predictor P_E is correct for ξ if for any k and any repetition procedure for E (giving parameters $\lambda_1, \lambda_2, \dots$ when E is repeated) there exists an $n \geq k$ such that after n repetitions of E producing the outputs $x_1, \dots, x_n$, the sequence of predictions $P_E(\xi(\lambda_1)), \dots, P_E(\xi(\lambda_n))$:

1. contains k correct predictions,
2. contains no incorrect prediction; e.g. the remaining $n-k$ predictions are withheld.

---

[1] If one insists on a discrete or computational universe—whether it be as a "toy" universe, in reality or in virtual reality—then λ could be conceived as a finite quantity. This is, however, the exception, and in the standard view of real physical experiments λ would be infinite, even if the prediction itself is discrete or finite.

From this notion of correctness we can define predictability both relative to a set of extractors, and in an absolute form.

Let Ξ be a set of extractors. An experiment E is *predictable for* Ξ if there exists a predictor P_E and an extractor $\xi \in \Xi$ such that P_E is correct for ξ. Otherwise, it is *unpredictable for* Ξ.

This means that P_E has access to an extractor $\xi \in \Xi$ which, when using this extractor to provide input to P_E, can be made to give arbitrarily many correct predictions by repeating E enough (but finitely many) times, without ever giving an incorrect prediction.

The more objective notion proposed in [2] can be recovered by considering all possible extractors. Specifically, an experiment is *(absolutely) predictable* if there exists a predictor P_E and an extractor ξ such that P_E is correct for ξ. Otherwise, it is (absolutely) unpredictable.

The outcome x of an *single trial* of the experiment E is *predictable (for* Ξ*)* if E is predictable (for Ξ). Otherwise, it is unpredictable (for Ξ). We emphasise here that the predictability of the result of a single trial is predictability *with certainty*.

B. Some remarks on relativisation

The absolute notion of predictability defined above is clearly the stronger notion, and it was for this notion that the unpredictability of quantum value indefiniteness was proved in [6]. However, beyond indeterminism, which offers the most obvious physical case for unpredictability, it is not simple to find physical properties which can guarantee unpredictability. This is a result of the stringent requirements the definition imposes: we must prove that no predictor-extractor pair exists satisfying the requirements of prediction. The inability to do so does not mean such phenomena are necessarily unpredictable, but only that we cannot often prove either way.

In some physical situations, particularly in classical physics, our inability to predict would seem to be linked to our epistemic lack of information—often due to measurement. Put differently, it is a result of only having access to a set Ξ of extractors of limited power. Our relativised model of prediction attempts to capture this, defining predictability relative to a given set of extractors Ξ.

1. *Choosing the set of extractors* Ξ

In defining this notion, we deliberately avoided saying anything about how Ξ should be specified. Here we outline two possible ways this can be done.

The simplest but most restrictive way would be to explicitly specify the set of extractors. As an example, let us consider the experiment of firing a cannonball from a cannon and the task of predicting where it will land (assume for now that the muzzle velocity is known and independent of firing angle). Clearly the position will depend on the angle the cannonball is fired at. Then if we are limited to measuring this with a ruler, we can consider, for example, the set of extractors

$$\Xi = \{\xi \mid \xi(\lambda) = (x,y) \text{ where } x \text{ and } y \text{ are the muzzle position to an accuracy of 1cm}\}$$

and then consider predictability with respect to this set Ξ. (For example, by using trigonometry to calculate the angle of firing, and then where the cannonball will land.)

Often it is unrealistic to characterise completely the set of extractors available to an agent in this way—think about a standard laboratory full of measuring devices that can be used in various ways. Furthermore, such devices might be able to measure properties indirectly, so we might not be able to characterise the set Ξ so naively. Nonetheless, this can allow simple consideration and analysis of predictability in various situations, such as under-sensitivity to initial conditions.

A more general approach, although often requiring further assumptions, is to limit the 'information content' of extractors. This avoids the difficulty of having to explicitly specify Ξ. Continuing with the same example as before, we could require that no extractor $\xi \in \Xi$ can allow us to know the firing angle better than 1°. This circumvents any problems raised by the possibility of indirect measurement, but of course requires us to have faith in the assumption that this is indeed the case; it could be possible that we *can* extract the angle better than this, but we simply don't know how to do it with our equipment. (This would not be a first in science!) Nonetheless, this approach captures well the epistemic position of the predicting agent.

Let us formalise this more rigorously. We hypothesise that we cannot do any better than a hypothetical extractor ξ' extracting the desired physical quantity. Then we characterise Ξ by asserting: for all $\xi \in \Xi$ there is no computable function f such that for every parameter λ, $f(\xi(\lambda))$ is more accurate than ξ'. Obviously, the evaluation of 'more accurate' requires a (computable) metric on the physical quantity extracted, something not unreasonable physically given that observables tend to be measured as rational numbers as approximations of reals [7].

This general approach would need to be applied on a case by case basis, given assumptions about the capabilities available to the predicting agent. Assumptions have to be carefully justified and, ideally, subject themselves to experimental verification.

Either of these approaches, and perhaps others, can be used with our relativised model of prediction. In any such case of relativisation, one would need to argue that the set Ξ unpredictability is proven for is relevant physically. This is unavoidable for any epistemic model of prediction.

2. A detailed example

Let us illustrate the use of relativised unpredictability with a more interesting example of an experiment which is predictable, but its intuitive unpredictability is well captured by the notion of relativised unpredictability. In particular, let us consider a simple chaotic dynamical system. Chaos is often considered to lead to unpredictability within a system. However, chaos is, formally, an asymptotic property [8], and we will see that as a result the unpredictability of chaotic systems is not so simple as might be initially suspected.

For simplicity, we will take the example of the dyadic map, i.e. the operation on infinite sequences defined by $d(x_1x_2x_3\dots) = x_2x_3\dots$, as in [2]. We work with this example since it is mathematically clear and simple, and is an archetypical example of a chaotic system, being topologically conjugate to many other well-known systems [9]. However, the analysis could equally apply to more familiar (continuous) chaotic physical dynamics, such as that of a double pendulum.

Let us consider the hypothetical experiment E_k (for fixed $k \geq 1$) which involves iterating the dyadic map k times (i.e. d^k) on an arbitrary 'seed' $\mathbf{x} = x_1x_2\dots$. The outcome of the experiment is then taken to be the first bit of the resulting sequence $d^k(\mathbf{x}) = x_{k+1}x_{k+2}\dots$, i.e. x_{k+1}. This corresponds to letting the system evolve for some fixed time k before measuring the result.

While the shift d (and hence d^k) is chaotic and generally considered to be unpredictable, it is clearly absolutely predictable if we have an extractor that can 'see' (or measure) more than k bits of the seed. That is, take the extractor $\xi_k(\lambda_{\mathbf{x}}) = x_{k+1}$ which clearly extracts only finite information, and the identity Turing machine I as P_{E_k} so that, for any trial of E_k with parameter $\lambda_{\mathbf{x}}$ we have $P_{E_k}(\xi_k(\lambda_x)) = I(x_{k+1}) = x_{k+1}$, which is precisely the result of the experiment.

On the other hand, if we consider that there is some limit l on the 'precision' of measurement of $\mathbf{x}$ that we can perform, the experiment is unpredictable relative to this limited set of extractors Ξ_l defined such that for every sequence $\mathbf{x}$, every computable function f there exists λ such that for all $j > l$, $f(\xi(\lambda)) \neq x_j$. It is clear that for $l = k$, *given the limited precision of measurements assumption*, the experiment E_k is unpredictable for Ξ_k. Indeed, if this were not the case, the pair (ξ, P_{E_k}) allowing prediction would make arbitrarily many correct predictions, thus contradicting the assumption on limited precision of measurements.

This example may appear somewhat artificial, but this is not necessarily so. If one considers the more physical example of a double pendulum, as mentioned earlier, one can let it evolve for a fixed time t and attempt to predict its final position (e.g. above or below the horizontal plane) given a set limit l on the precision of any measurement of the initial position in phase space. If the time t is very short, we may well succeed, but for long t this becomes unpredictable.

This re-emphasises that chaos is an asymptotic property, occurring only strictly at infinite time. While in the limit it indeed seems to correspond well to unpredictability, in finite time the unpredictability of chaotic systems is relative: a result of our limits on measurement. Of course, in physical situations such limits may be rather fundamental: thermal fluctuation or quantum uncertainty seem to pose very real limits on measurement precision [7], although in most situations the limits actually obtained are of a far more practical origin.

III. UNPREDICTABILITY IN QUANTUM MECHANICS

For a long time and under the guidance of the standard Copenhagen interpretation of quantum mechanics, the outcomes of individual quantum measurements have been viewed within (and beyond) the community as inherently unpredictable. This has become more evident and more important with the recent surge of quantum information theory, where quantum randomness plays a key role. In particular, its use in randomness generation [4, 10], cryptography [11], and computing means the status of quantum unpredictability is no longer only an issue for physicists set on understanding the theory; it is also an issue of practical importance.

Historically, this was a belief about the quantum world, corroborated by empirical results and hypotheses. It is of interest to ask if such unpredictability can be more formally based on deeper principles within quantum theory, helping elucidate the situation of quantum measurements.

Value indefiniteness, a formalised notion of indeterminism, appears to be one of the most promising means to certify unpredictability. Since we have discussed in detail the notion of value indefiniteness previously [3], we will just summarise the basic concept and its relation to unpredictability.

A. Quantum value indefiniteness

Value indefiniteness is the notion that the outcomes of quantum measurements are not predetermined by any function of the observables and their measurement contexts—that there are no hidden variables. It is thus a formalised notion of indeterminism, and the measurement of such observables results in an outcome not determined before the measurement took place.

While it is possible to hypothesise value indefiniteness in quantum mechanics [12], its importance comes from the fact that it can be proven (for systems represented in dimension three or higher Hilbert space) to be true under simple classical hypotheses via the Kochen-Specker theorem [3, 13, 14]. We will not present the formalism of the Kochen-Specker theorem here, but just emphasise that this gives value indefiniteness a more solid status than a blind hypothesis in the face of a lack of deterministic explanation for quantum phenomena.

Intuitively, value indefiniteness seems a good candidate for giving rise to absolute unpredictability. Since the measurement outcomes are not predetermined, our inability to predict their outcomes does not seem to be from merely epistemic limitations on our knowledge of the state. In [2] we proved that this is indeed the case in our model of unpredictability: *If E is an experiment measuring a quantum value indefinite projection observable, then the outcome of a single trial of E is (absolutely) unpredictable.* Hence, value indefiniteness can indeed guarantee absolute unpredictability. However, as we mentioned, its applicability to quantum mechanical reality relies largely on, and is thus relative to, the Kochen-Specker theorem and its hypotheses [3, 13, 14], which only holds for systems in three or more dimensional Hilbert space.

B. Complementarity

The quantum phenomena of complementarity has also been linked to unpredictability and, contrary to the value indefiniteness pinpointed by the Kochen-Specker theorem, is present in all quantum systems. By itself quantum complementarity is not *a priori* incompatible with value definiteness (there exist automaton and generalised urn models featuring complementarity but not value indefiniteness [15, 16]) and hence constitutes a weaker hypothesis, even though it is sometimes taken as 'evidence' when arguing that value indefiniteness is present in all quantum systems.

It is therefore of interest to see if complementarity alone can guarantee some degree of unpredictability. This interest is not only theoretical, but also practical as some current quantum random generators, such as Quantis [17], operate in two-dimensional Hilbert space where the Kochen-Specker theorem cannot be used to certify value indefiniteness, and would hence seem to (implicitly) rely on complementarity for certification.

1. Quantum complementarity

Let us first discuss briefly the notion of quantum complementarity, before we proceed to an analysis of its predictability.

The principle of complementarity was originally formulated and promoted by Pauli [18]. It is indeed more of a general principle rather than a formal statement about quantum mechanics, and states that it is impossible to simultaneously measure formally non-commuting observables, and for this reason commutativity is nowadays often synonymous with co-measurability. It is often discussed in the context of the position and momentum observables, but it is equally applicable to any other non-commuting observables such as spin operators corresponding to different directions, such as S_x and S_y, which operate in two-dimensional Hilbert space.

Given a pair of such "complementary" observables and a spin-$\frac{1}{2}$ particle, measuring one observable alters the state of the particle so that the measurement of the other observable can no longer be performed on the original state. Such complementarity is closely related to Heisenberg's original uncertainty principle [19], which postulated that any measurement arrangement for an observable necessarily introduced uncertainty into the value of any complementary observable. For example, an apparatus used to measure the position of a particle, would necessarily introduce uncertainty in the knowledge of the momentum of said particle. This principle and supposed proofs of it have been the subject of longstanding (and ongoing) debate [20–22].

More precise are the formal uncertainty relations due to Robertson [23]—confusingly also often referred to as Heisenberg's uncertainty principle—which state that the standard deviations of the position and momentum observables satisfy $\sigma_x\sigma_p \geq \hbar/2$, and give a more general form for any non-commuting observables A and B. However, this mathematically only places constraints on the variance of repeated measurements of such observables, and does not formally imply that such observables cannot be co-measured, let alone have co-existing definite values, as is regularly claimed [24, Ch. 3].

Nonetheless, complementarity is usually taken to mean the stronger statement that it is impossible to simultaneously measure such pairs of observables, and that such measurement of one will result in a loss of information relating to the non-measured observable following the measurement. We will take this as our basis in formalising contextuality, but we do not claim that such a loss of information need be more than epistemic; to deduce more from the uncertainty relations one has to assume quantum indeterminism—that is, value indefiniteness.

2. Complementarity and value definiteness: a toy configuration

In order to illustrate that complementarity is not incompatible with value definiteness we briefly consider an example of a toy-model of a system that is value definite but exhibits complementarity. This model was outlined in [16] and concerns a system modelled as an automaton; a different, but equivalent, generalised urn-type model is described in [15].

The system is modelled as a *Mealy automaton* $\mathcal{A} = (S, I, O, \delta, W)$ where S is the set of states, I and O the input and output alphabets, respectively, $\delta : S \times I \to S$ the transition function and $W : S \times I \to O$ the output function. If one is uncomfortable thinking of a system as an automaton, one can consider the system as a black-box, whose internal workings as an automaton are hidden. The state of the system thus corresponds to the state s of the automaton, and each input character $a \in I$ corresponds to a measurement, the output of which is $W(s,a)$ and the state of the automaton changes to $s' = \delta(s,a)$. To give a stronger correspondence to the quantum situation, we demand that repeated measurements of the same character $a \in I$ (i.e. observable) gives the same output: for all $s \in S$ $W(s,a) = W(\delta(s,a),a)$. The system is clearly value definite, since the output of a measurement is defined prior to any measurement being made.

However, if we have two 'measurements' $a, b \in I$ such that $W(s,a) \neq W(\delta(s,b),a)$ then the system behaves contextually; a and b do not commute. Measuring b changes the state of the system from s to $s' = \delta(s,b)$, and we lose the ability to know $W(s,a)$.

While this example is not intended to realistically model quantum mechanics, it represents well many aspects of quantum logic, and serves to show that contextuality itself is not incompatible with value definiteness.

3. Complementarity as an argument for value indefiniteness

While complementarity is not incompatible with value definiteness, it is worth briefly discussing whether it nonetheless provides good evidence of quantum value indefiniteness.

On its own, complementarity tells us that we cannot obtain via measurement a pre-existing value for certain observables. The choice of whether to interpret this as being due to the actual non-existence of these parameters or not, could be seen as a choice of faith between determinism and indeterminism. Einstein famously preferred to stick to a deterministic explanation, while his contemporaries were more willing to take the bold move of attributing the seemingly unpredictable results of quantum measurements to indeterminism.

This perhaps changed as a result of the Bell and Kochen-Specker theorems [13, 25], which showed, at least in dimension three or higher Hilbert space, that value indefiniteness is much more difficult to avoid. With such evidence for value indefiniteness in quantum mechanics, this could be interpreted as swinging the battle of faith between determinism and indeterminism towards the latter and leading more naturally to an interpretation of complementarity along these lines.

However, since this reasoning relies indirectly on the Kochen-Specker theorem, our confidence in value indefiniteness in two-dimensional Hilbert spaces—as are utilised in various quantum random number generators [4, 17]—remains weaker than in higher dimensional systems.

C. Complementarity and unpredictability

Complementarity tends to be more of a general principle than a formal statement, hence in order to investigate mathematically the degree of unpredictability that complementarity entails we need to give complementarity a solid formalism. While several approaches are perhaps possible, following our previous discussion we choose a fairly strong form of complementarity and consider it not as an absolute impossibility to simultaneously know the values of non-commuting observables, but rather as a restriction on our current set of extractors—i.e. using standard quantum measurements and other techniques we currently have access to.

Formally, we say the set of extractors Ξ is *protected for* (A,B) *by complementarity* if there does not exist an extractor $\xi \in \Xi$ and a computable function f such that, whenever the value $v(A)$ of an observable A is known,[2] then for all λ $f(\xi(\lambda)) = v(B)$, where B is any quantum observable not commuting with A, i.e. $[A,B] \neq 0$. If the observables (A,B) are evident from the context, we will often simply say that Ξ is protected by complementarity.

[2] We assume for simplicity that the observables A and B have discrete spectra (as for bounded systems), i.e., the eigenvalues are isolated points, and hence the values $v(A)$ and $v(B)$ can be uniquely determined by measurement. Furthermore, since the choice of units is arbitrary (e.g., we can choose $\hbar = 1$) one can generally assume that $v(A)$ (and $v(B)$) are rational-valued, and hence can be known 'exactly'. Even if this were not the case, a finite approximation of $v(A)$ is sufficient to uniquely identify it, and thus enough here.

For continuous observables it is obviously impossible to identify precisely $v(A)$ or $v(B)$. Such systems are generally idealisations, but one can still handle this case by considering observables A' and B' that measure A and B to some fixed accuracy. Protection by complementarity may depend on this accuracy. For example, for position and momentum, one expects complementarity to apply only when the product of accuracies in position and momentum is less than $\hbar/2$ according to the uncertainty relations.

This states that, if we know $v(A)$ we have no way of extracting, directly or indirectly, the value $v(B)$ without altering the system. We stress that this doesn't imply that A and B cannot simultaneously have definite values, simply that we cannot *know* both at once.

Let us consider an experiment E that prepares a system in an arbitrary pure state $|\psi\rangle$, thus giving $v(P_\psi) = 1$ for the projection observable $P_\psi = |\psi\rangle\langle\psi|$, before performing a projective measurement onto a state $|\phi\rangle$ with $0 < \langle\psi|\phi\rangle < 1$ (thus $[P_\psi, P_\phi] \neq 0$) and outputting the resulting bit.

It is not difficult to see that if Ξ is protected for (P_ψ, P_ϕ) by complementarity—i.e. if the predicting agent is limited by the above power—then the outcome of E is unpredictable for Ξ. For otherwise, there would exist an extractor $\xi \in \Xi$ and a computable predictor P_E such that, under any repetition procedure giving parameters $\lambda_1, \lambda_2, \dots$ we have $P_E(\xi(\lambda_i)) = x_i$ for all i, where x_i is the outcome of the ith iteration/trial. But if we take $f = P_E$, then the pair (ξ, f) contradicts the protection by complementarity, and hence E is unpredictable for Ξ.

If is important to note that this result holds regardless of whether the observables measured are value definite or not, although the value definite case is of more interest. Indeed, if the observables are value indefinite then we are guaranteed unpredictability without assuming protection by complementarity.

As a concrete example, consider the preparation of a spin-$\frac{1}{2}$ particle, for instance an electron, prepared by in a $S_z = +\hbar/2$ state before measuring the complementary observable $2S_x/\hbar$ generating the outcome $\{-1, +1\}$. This could, for example, be implemented by a pair of orthogonally aligned Stern-Gerlach devices. Next let us assume that the system is indeed value definite. The preparation step means that, prior to the trial of the experiment being performed, $v(S_z)$ is known, and by assumption $v(S_x)$ exists (i.e. is definite) and is thus "contained" in the parameter λ. The assumption that Ξ is protected by complementarity means that there is no extractor $\xi \in \Xi$ able to be used by a predictor P_E giving $P_E(\xi(\lambda_i)) = 2v(S_x)/\hbar = x_i$, thus giving unpredictability for Ξ.

As we noted at the start of the section, this is a fairly strong notion of complementarity (although not the strongest possible). A weaker option would be to consider only that we cannot directly extract the definite values: that there is no $\xi \in \Xi$ such that $\xi(\lambda) = v(S_x)$ for all λ. However, this does not rule out the possibility that there are other extractors allowing us to indirectly measure the definite values (unless we take the strong step of assuming Ξ is closed under composition with computable function, for example). This weaker notion of complementarity would thus seem insufficient to derive unpredictability for Ξ, although it wouldn't show predictability either. We would thus, at least for the moment, be left unsure about the unpredictability of measurement protected by this weak notion of complementarity.

IV. UNPREDICTABILITY AND COMPUTABILITY

It has previously been shown that, subject to certain physical assumptions (as is always the case), quantum value indefiniteness leads to a strong form of incomputability[3] in sequences produced by repeated measurements of such observables [3]. Having developed a model of unpredictability based on the ability to predict via computational means under which such quantum measurement are unpredictable, it is worthwhile briefly discussing the relationship between unpredictability and computability. We have discussed this relation in the context of absolute unpredictability previously [2], but here we consider this in the light of relativised unpredictability and complementarity.

A. (Relativised) unpredictability

This relation between value indefiniteness and incomputability may lead one to pose the question of whether such a result holds for any absolutely unpredictable experiment. However, in [2] we showed that this is not the case: there are absolutely unpredictable experiments capable of producing both computable and strongly incomputable sequences when repeated *ad infinitum*.

These results shows, *a fortiori*, that the same is true for relativised unpredictability. Since an absolutely unpredictable experiment is also unpredictable for any subset of extractors, there also exist experiments capable of producing computable outcomes in the limit which are unpredictable for a restricted sets of extractors.

B. Incomputability and complementarity

Even though the (relativised) unpredictability associated with complementary quantum observables cannot guarantee incomputability, one may ask whether this complementarity may, with reasonable physical assumptions, lead directly to incomputabil-

[3] Technically: A sequence $x_1x_2\dots$ is bi-immune if it contains no computable subsequence.

ity, much as value indefiniteness does.

We will show that complementarity, unlike value indefiniteness, cannot guarantee any kind of incomputability. Specifically, we will show how an, admittedly toy, (value definite) system exhibiting complementarity (and thus relatively unpredictable) can produce computable sequences when repeated.

Consider an experiment E involving the prediction of the outcome of measurements on an (unknown) Mealy automaton $M = (S, I, O, \delta, W)$, which we can idealise as a black-box, with $\{x, z\} \in I$ characters in the input alphabet, output alphabet $O = \{0, 1\}$ and satisfying the condition that x and z are complementary: that is, for all $s \in S$ we have $W(s, z) \neq W(\delta(s, x), z)$ and $W(s, x) \neq W(\delta(s, z), x)$. This automaton is deliberately specified to resemble measurements on a qubit. This very abstract model can be viewed as a toy interpretation of a two-dimensional quantum, value definite system, where the outcome of measurements are determined by some unknown, hidden Mealy automaton. Since the Kochen-Specker theorem does not apply to two-dimensional systems, this value definite toy model poses no direct contradiction with quantum mechanics, even if it is not intended to be particularly realistic. We complete the specification of E by considering a trial of E to be the output on the string xz, i.e., if the automaton is initially in the state s, the output is $W(\delta(s, x), z)$, and the final state is $\delta(\delta(s, x), z)$. This is a clear analogy to the preparation and measurement of a qubit using complementary observables, of the type discussed earlier.

Let us show that E is unpredictable for a set Ξ of extractors that expresses the protection by complementarity present in Mealy automata. In particular, let us consider the set Ξ that, in analogy to the protection by complementarity of two quantum observables defined earlier, is protected by complementarity for the inputs $x, z \in I$ in the following sense: *there is no extractor $\xi \in \Xi$ and computable function f such that, if λ_M is the state of a system with Mealy automaton M in a state s such that $\delta(s, x) = s$ (or $\delta(s, z) = s$, i.e., in an 'eigenstate' x or z), then $f(\xi(\lambda_M)) = W(s, z)$ (or $f(\xi(\lambda_M)) = W(S, x)$).* That is, if M is in an 'eigenstate' of x, we cannot extract the output of the input z (and similarly for z and x interchanged).

Let us assume for the sake of contradiction that E is predictable for Ξ: i.e., there is a predictor P_E and extractor $\xi \in \Xi$ such that E is predictable for Ξ. Thus, from the definition of predictability, the pair (P_E, ξ) must provide infinitely many correct predictions when repeated with the following iterative procedure (in analogy to preparing in an x eigenstate): the black-box containing M is prepared by inputting 'x', and then the experiment is run and the output recorded. The next repetition is performed on the same system, preparing the box once again by inputting 'x' and performing the experiment. Thus, from the definition of Mealy automata, for each repetition i the automaton M is in a state s_i such that $\delta(s_i, x) = s_i$ before the ith trial is performed. Thus, the output of the ith trial of E is precisely $W(\delta(s_i, x), z) = W(s_i, z)$, and for each trial we have $P_E(\xi(\lambda_i)) = W(s_i, z)$, but since P_E is a computable function this predictor/extractor pair contradicts the protection by complementarity of Ξ, and hence we conclude that E is unpredictable for Ξ.

The main question is thus the (in)computability of sequences produced by the concatenation of outputs from infinite repetitions of E. The experiment can be repeated under many different repetition scenarios, but the simplest is by performing the experiment again on the same black-box (and thus with the same automaton) with the final state of M becoming the initial state for the next repetition. In this case, the sequence produced is computable—even cyclic—as a result of the automaton M used. Thus, even if this is not the case under all repetition scenarios, we cannot guarantee that the sequence produced is incomputable, even though E is unpredictable with respect to Ξ.

We note that one could easily consider slightly more complicated scenarios where the outcomes are controlled not by a Mealy automaton, but an arbitrary computable—or even, in principle, incomputable—function; complementarity is agnostic with respect to the computability of the output of such an experiment. Such a computable sequence may be obviously computable—e.g. $000\ldots$, but it could equally be something far less obvious, such as the digits in the binary expansion of π at prime indices, e,g, $\pi_2\pi_3\pi_5\pi_7\pi_{11}\ldots$ Hence, this scenario cannot be easily ruled out empirically, regardless of the computability, that is, low complexity, of the resulting sequences. Further emphasising this, we note that computable sequences can also be Borel-normal, as in Champernowne's constant or (as conjectured) π, and thus satisfy many statistical properties one would expect of random sequences.

Our point was not to propose this as a realistic physical model—although it perhaps cannot be dismissed so easily—but to illustrate a conceptual possibility. Value indefiniteness rules this computability out, but complementarity fails to do the same in spite of its intuitive interpretation as a form of quantum uncertainty. At best it can be seen as an epistemic uncertainty, as it at least poses a physical barrier to the knowledge of any definite values. The fact that complementarity cannot guarantee incomputability is in agreement with the fact that value definite, *contextual* models of quantum mechanics are perfectly possible [2, 26]; such models need not contradict any principle of complementarity, and can be computable or incomputable.

C. Means relative versus absolute models

In considering the unpredictability of measurements of complementary quantum observables, we made the explicit decision to consider complementarity as a restriction on the set of extractors Ξ available to a given predicting agent, but not as an *absolute* limit on possible extractors. One could consider this stronger approach and hypothesis that no such extractor ξ extracting complementary values can physically exist *for any set Ξ of extractors*. However, in the case of value definiteness protected by complementarity (the main case of interest), this would mean the existence of definite values that are *in principle* unknowable—a strongly metaphysical assumption that is by its very nature untestable.

In this approach complementarity would guarantee *absolute* unpredictability (i.e. not just relativised). Indeed, the definition of an extractor requires that it be physically reasonable. However, while this would provide absolute unpredictability, as we discussed in Section IV B, this still provides no guarantee of incomputability on its own.

V. SUMMARY

In this paper we used a formal model of relativised unpredictability for physical systems—which we developed within—to investigate the relation between complementarity and unpredictability, and in particular whether quantum complementarity alone entails the unpredictability of quantum measurement outcomes.

In contrast to the use of quantum value indefiniteness to certify the unpredictability of measurements, complementarity alone is not, *a priori*, incompatible with value definiteness and determinism. We illustrated this fact with some specific toy examples using Mealy automata, discussed how this could be extended to more physically "realistic" models, and studied the compatibility with value definite contextual models of quantum mechanics.

We showed that, unlike measurements certified by value indefiniteness, those certified by complementarity alone are not necessarily absolutely unpredictable: *they are unpredictable relative to the ability of the predicting agent to access the values of complementarity observables*—a more epistemic, relativised notion of predictability. This is a general result about complementarity, not specifically in quantum mechanics, and certification by complementarity and value indefiniteness need not be mutually exclusive. Indeed, in dimension three and higher Hilbert space, relative to the assumptions of the Kochen-Specker theorem [3] one has certification by both properties, value indefiniteness thus proving the stronger certification. However, our results are of more importance for two-dimensional systems, since although quantum complementarity is present, this does not necessarily lead to value indefiniteness. While one may postulate value indefiniteness in such cases as well, this constitutes an extra physical assumption, a fact which should not be forgotten [2]. In assessing the randomness of quantum mechanics, one thus needs to take carefully into account all physical assumptions contributing towards the conclusions that one reaches.

Finally we summarise the relation between the various notions of unpredictability and properties of systems that we discussed. Quantum value indefiniteness implies the absolute unpredictability of measurement outcomes, which in turn ensure the unpredictability of such measurements relative to any observer; the converse implications do not hold in general. Value indefiniteness, as was previously shown [2], implies the incomputability of sequences generated by measuring value indefinite observables, a property that is not true in general for absolutely unpredictable experiments, and hence also for relatively unpredictable experiments. We illustrated these implications in detail with examples involving both classical chaotic maps, Mealy automata, and toy models of simple quantum systems. Of particular interest is the fact that complementarity does not guarantee absolute unpredictability, nor the incomputability of sequences generated by measuring complementary observables and concatenating their outcomes. This means that quantum value indefiniteness and the Kochen-Specker theorem appear, for now, essential in certifying the unpredictability and incomputability of quantum randomness.

ACKNOWLEDGMENTS

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] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, "On the unpredictability of individual quantum measurement outcomes," (2014), CDMTCS report series 458, arXiv:1403.2738.

[3] 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.

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

[5] B. Jack Copeland, "The church-turing thesis," in *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta (2008) fall 2008 ed.

[6] C.S. Calude A.A. Abbott and K. Svozil, *On the Unpredictability of Individual Quantum Measurement Outcomes*, Report CDMTCS-458 (Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, 2014).

[7] Giuseppe Longo and Thierry Paul, "The mathematics of computing between logic and physics," (2010).

[8] Thierry Paul, "Semiclassical analysis and sensitivity to initial conditions," Information and Computation **207**, 660–669 (2009).

[9] Robert L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed. (Addison-Wesley, Redwood City, CA, 1989).

[10] 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).

[11] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum cryptography," Review of Modern Physics **74**, 145–195 (2002).

[12] Anton Zeilinger, "A foundational principle for quantum mechanics," Foundations of Physics **29**, 631–643 (1999).

[13] 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).

[14] Itamar Pitowsky, "Infinite and finite Gleason's theorems and the logic of indeterminacy," Journal of Mathematical Physics **39**, 218–228 (1998).

[15] Ron Wright, "Generalized urn models," Foundations of Physics **20**, 881–903 (1990).

[16] Karl Svozil, "Logical equivalence between generalized urn models and finite automata," International Journal of Theoretical Physics **44**, 745–754 (2005), arXiv:quant-ph/0209136.

[17] ID Quantique SA, *QUANTIS. Quantum number generator* (idQuantique, Geneva, Switzerland, 2001-2009).

[18] Wolfgang Pauli, "Die allgemeinen Prinzipien der Wellenmechanik," in *Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I*, edited by S. Flügge (Springer, Berlin, Göttingen and Heidelberg, 1958) pp. 1–168.

[19] Werner Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," Zeitschrift für Physik **43**, 172–198 (1927).

[20] Paul Busch, Pekka Lahti, and Reinhard F. Werner, "Measurement uncertainty relations," Journal of Mathematical Physics **55**, 042111 (2014).

[21] Ron Cowen, "Proof mooted for quantum uncertainty," Nature News **498**, 419–420 (2013).

[22] Lee A. Rozema, Ardavan Darabi, Dylan H. Mahler, Alex Hayat, Yasaman Soudagar, and Aephraim M. Steinberg, "Violation of Heisenberg's measurement-disturbance relationship by weak measurements," Physical Review Letters **109**, 100404 (2012).

[23] H. P. Robertson, "The unvertainty principle," Physical Review **34**, 163–164 (1929).

[24] Karl R. Popper, *Quantum Theory and the Schism in Physics* (Routledge, 1992).

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

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