

Article

A Non-Probabilistic Model of Relativised Predictability in Physics

Alastair A. Abbott ^{1,2,3,*}, Cristian S. Calude ¹ and Karl Svozil ^{1,4}

¹ Department of Computer Science, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand; E-Mail: cristian@cs.auckland.ac.nz

² Centre Cavallès, République des Savoirs, USR 3608, CNRS, Collège de France and École Normale Supérieure, 29 rue d’Ulm, 75005 Paris, France

³ Institut Néel, CNRS and Université Grenoble Alpes, 38042 Grenoble Cedex 9, France

⁴ Institute for Theoretical Physics, Vienna University of Technology, Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria; E-Mail: svozil@tuwien.ac.at

* Author to whom correspondence should be addressed; E-Mail: a.abbott@auckland.ac.nz.

Academic Editors: Mark Burgin and Wolfgang Hofkirchner

Received: 30 September 2015 / Accepted: 12 November 2015 / Published: 19 November 2015

Abstract: Unpredictability is an important concept throughout physics and plays a central role in quantum information theory. Despite this, little effort has been devoted to studying generalised notions or models of (un)predictability in physics. In this paper, we continue the programme of developing a general, non-probabilistic model of (un)predictability in physics. We present a more refined model that is capable of studying different degrees of “relativised” unpredictability. This model is based on the ability of an agent, acting via uniform, effective means, to predict correctly and reproducibly the outcome of an experiment using finite information extracted from the environment. We use this model to study the degree of unpredictability certified by different quantum phenomena further, showing that quantum complementarity guarantees a form of relativised unpredictability that is weaker than that guaranteed by Kochen–Specker-type value indefiniteness. We exemplify further the difference between certification by complementarity and value indefiniteness by showing that, unlike value indefiniteness, complementarity is compatible with the production of computable sequences of bits.

Keywords: prediction; unpredictability; randomness; complementarity

1. Introduction

Many physical processes and phenomena are intuitively thought of as unpredictable: the roll of a die, the evolution of weather systems and the outcomes of quantum measurements, to mention a few. While *ad hoc* definitions of unpredictability may exist within certain domains, little work has been done towards developing a more general understanding of the concept. Although domain-specific notions of unpredictability may help describe and categorise phenomena within the domain, the concept of unpredictability has a much more central and important role in quantum information theory.

Many of the advantages promised by quantum information theory and cryptography rely critically on the belief that the outcomes of quantum measurements are intrinsically unpredictable [1,2]. This belief underlies the use of quantum random number generators to produce “quantum random” sequences that are truly unpredictable (unlike pseudo-randomness) [3], as well as the generation of cryptographic keys unpredictable to any adversary [2]. Such claims of quantum unpredictability are generally based on deeper theoretical results, such as the Kochen–Specker [4] and Bell [5] theorems, or quantum complementarity, but nonetheless remain informal intuition.

The quantum cryptography community has used a probability theoretic approach to try and make use of, and quantify, the degree of unpredictability in quantum information-theoretical situations, in particular by following the cryptographic paradigm of adversaries with limited side information [6]. This approach, while suitable in such cryptographic situations precisely because of its epistemic nature [7], relies on the probabilistic formalism of quantum mechanics and the subsequently assumed unpredictability. In order to fully understand and study the degree of quantum unpredictability and randomness, it is instead crucial to have more general models of unpredictability to apply.

Historically, little work has been devoted to such generalised notions of unpredictability. In [8], we discussed in some detail the most notable approaches, in particular those of Popper [9], Wolpert [10] and Eagle [11]. In response to these approaches, we outlined a new model based on 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.

This model allowed us to consider a specific, ontic form of unpredictability, which was particularly suited for analysing the type of unpredictability quantum mechanics claims to provide. However, this strong form of unpredictability is too strong in many cases and failed to capture the possible different degrees of unpredictability: what is predictable for one agent may not be for another with different capabilities.

In this paper, we refine and improve this model of (un)predictability, providing a more nuanced, relativised notion of unpredictability that can take into account the epistemic limits of an observer, something crucial, for example, in chaotic systems [12]. This also provides the ability to look at the degree of unpredictability guaranteed by different possible origins of quantum unpredictability. We examine one such case, that of quantum complementarity, in detail and show that it provides a weaker form of unpredictability than that arising from Kochen–Specker-type value indefiniteness, as discussed in [8].

2. Relativised Model of Predictability

The model of (un)predictability that we proposed in [8] is based on the ability of an agent to, in principle, predict the outcome of a physical experiment. By using computability theory, motivated by the Church–Turing thesis, to provide a universal framework in which prediction can occur; this information-theoretical approach allows different physical systems and theories to be uniformly analysed.

Here, we refine and extend this model in order to be able to relativise it with respect to the means/resources of the predicting agent. 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 such abilities.

Before we proceed to present our model in detail, we will briefly outline the key elements comprising it.

- (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 that we will justify further.
- (3) An extractor ξ , which 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, the measurement of some parameter, the iteration of the experiment, *etc.*
- (4) A prediction made by the agent with access to a set Ξ of extractors. The set of extractors Ξ provides the relativisation of the model.

This model is explicitly a non-probabilistic one, a fact that may seem overly restrictive given that highly probable events seem predictable. However, the uncertainty present in “high probabilities” represents an important latent unpredictability in such processes, and certainty is needed if predictions are to be related to definite properties of physical systems [13], as is the case in quantum scenarios, for example.

It should be noted that our model does not assess the ability to make statistical predictions about physical processes (about the throw of a die, for example), as probabilistic models might, but rather, the ability to predict precise measurement outcomes.

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

2.1. 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, that is the value to be predicted, is a single bit: zero or one. However, this can readily be generalised for any finite number of outcomes. 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, cannot 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 by the experimenter within their limited capacities, making use, for example, of the pertinent symmetries to describe the experiment. 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 be “an infinite quantity”, for example, an infinite sequence or a real number, structured in an unknown manner. (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 of as a finite quantity. This is, however, the exception, and in the orthodox view of real physical experiments, λ would be infinite, even if the prediction itself is discrete or finite, so we will adopt this view here.) 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 takes place, 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 zero, one 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. This is necessary to avoid the possibility that the predictor affects the very outcome the it is trying to predict.

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 choice of computability is motivated by the Church–Turing thesis, a rather robust assumption [14].

Extractor: An extractor is a physically-realizable device that a predicting agent can use to extract (a finite amount of) useful data that may not be a part of the description of E from λ to use for prediction, that is 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 produces a finite string of bits $\xi(\lambda)$ that can be physically realised without altering the system, that is passively. In order to be used by P_E for prediction, $\xi(\lambda)$ should be finite and effectively codable, for example 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 that 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; that is, the remaining $n - k$ predictions are withheld.

From this notion of correctness, we can define predictability both relative to a set of extractors and in a more 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 [8] can be recovered by considering all possible extractors. Specifically, an experiment is (simply) predictable if there exists a predictor P_E and an extractor ξ , such that P_E is correct for ξ . Otherwise, it is (simply) unpredictable.

The outcome x of a single trial of the experiment E performed with parameter λ is predictable (for Ξ) if E is predictable (for Ξ) and $P_E(\xi(\lambda)) = x$. Otherwise, it is unpredictable (for Ξ). We emphasise here that the predictability of the result of a single trial is predictability with certainty.

2.2. Relativisation

While the notion of simple predictability provides a very strong notion of unpredictability, one that seems to correspond to what is often meant in the context of quantum measurements [8], 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, unpredictability 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 .

2.2.1. Specifying 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 at which the cannonball is fired. Then, if we are limited to measuring this with a ruler, we can consider, for example, the set of extractors:

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

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 do not know how to do it with our equipment (which would not be a first in science). Nonetheless, this approach captures the epistemic position of the predicting agent well.

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 approximations of reals [15].

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 for which unpredictability is proven is relevant physically. This is unavoidable for any epistemic model of prediction.

2.2.2. A Detailed Example

Let us illustrate the use of relativised unpredictability with a more interesting example of an experiment that 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 be a form of unpredictability and is characterised by sensitivity to initial conditions and the mixing of nearby dynamical trajectories [12]. However, chaos is, formally, an asymptotic property [16], 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, that is the operation on infinite sequences defined by $d(x_1x_2x_3\dots) = x_2x_3\dots$, as in [8]. 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 [17]. 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 $d^k(\mathbf{x}) = x_{k+1}x_{k+2}\dots$, that is 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 simply 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 $P_{E_k}(\xi_k(\lambda_{\mathbf{x}})) = I(x_{k+1}) = x_{k+1}$, 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} and 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 of the 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 fluctuations or quantum uncertainty seem to pose very real limits on measurement precision [15], although in most situations, the limits actually obtained are of a far more practical origin.

3. Unpredictability in Quantum Mechanics

As we discussed in the Introduction, the outcomes of individual quantum measurements are generally regarded as being inherently unpredictable, a fact that plays an important practical role in quantum information theory [18,19]. This unpredictability has many potential origins, of which quantum value indefiniteness is perhaps one of the most promising candidates to be used to certify it more formally.

3.1. 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 [20], 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 [4,21,22]. 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.

In [8], we used our model to prove that value indefiniteness can indeed be used to explain quantum unpredictability. Specifically, we showed that if E is an experiment measuring a quantum value indefinite projection observable, then the outcome of a single trial of E is (simply) unpredictable.

Although value indefiniteness guarantees unpredictability, it relies largely on, and is thus relative to, the Kochen–Specker theorem and its hypotheses [4,21,23], which only holds for systems in three or more dimensional Hilbert space. It is thus useful to know if any other quantum phenomena can be used to certify unpredictability that would be present in two-dimensional systems or in the absence of other Kochen–Specker hypotheses and, if so, what degree of unpredictability is guaranteed.

3.2. 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 with at least two outcomes.

Although complementarity is often taken to refer to a range of different concepts [24], these are all closely related and are not *a priori* incompatible with value definiteness (there exist automaton and generalised urn models featuring complementarity, but not value indefiniteness [25,26]), and it hence constitutes a weaker hypothesis, even though it is occasionally taken as “evidence” when arguing that value indefiniteness is present in all quantum systems.

It is therefore of interest to see if a form of complementarity alone can guarantee some degree of unpredictability and is an ideal example to which to apply our model. This interest is not only theoretical, but also practical, as some current quantum random generators [3] 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.

3.2.1. Quantum Complementarity

Since complementarity can be taken to mean a range of different concepts [24], it is important that we first discuss briefly the notion of quantum complementarity and the particular form that we will use, before we proceed to an analysis of its predictability.

The principle of complementarity was originally formulated and promoted by Pauli [27]. As originally intended, it is more of a general principle than a formal statement about quantum mechanics and states that it is impossible to simultaneously (*i.e.*, jointly) measure formally non-commuting observables; 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 [28], which postulated that any measurement arrangement for an observable necessarily introduces 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 long-standing (and ongoing) debate [29–31].

More precise are the formal uncertainty relations due to Robertson [32], 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 variances 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 often claimed ([33], Chapter 3).

In contrast to such uncertainty relations, complementarity is usually taken to mean the stronger statement that it is impossible to simultaneously measure pairs of non-commuting observables and that a measurement of one will result in an irreversible loss of information relating to the other, non-measured, observable. Although one may define simultaneous (or joint) measurability in several ways, such as the existence of a joint distribution or the non-existence of uncertainty relations [24], we take this to mean the possibility to measure two observables A and B , such that subsequent measurements of either A or B yield the same results (*i.e.*, the state is not altered). We will take the negation of this as our basis in formalising complementarity, 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.

3.2.2. 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 [26] and concerns a system modelled as an automaton; a different, but equivalent, generalised urn-type model is described in [25].

In this framework, a quantum system is modelled as a Mealy automaton, and every input to the automaton, corresponding to a measurement, produces an outcome depending on the input and the internal state of the automaton, and may lead to an irreversible change in its state. If one is uncomfortable thinking of a quantum system as an automaton, one can consider the system as a black-box accessible only via inputs (measurements) and outputs (measurement results), whose internal workings as an automaton are hidden. Although such a model does not capture all of the behaviour of a quantum system, it represents many aspects of quantum logic well and, in particular, complementarity.

More formally, the system is modelled as a Mealy automaton $M = (Q, \Sigma, \Theta, \delta, \omega)$, where Q is the set of states, Σ and Θ the input and output alphabets, respectively, $\delta : Q \times \Sigma \rightarrow Q$ the transition function and $\omega : Q \times \Sigma \rightarrow \Theta$ the output function. The state q of the automaton thus represents a hidden internal state of the system, and each input character $a \in \Sigma$ corresponds to a measurement, the output of which is $\omega(q, a)$; the state of the automaton changes to $q' = \delta(q, a)$. To give a stronger correspondence to the quantum situation, a further condition is required: that repeated measurements of the same input $a \in \Sigma$ (*i.e.*, observable) give the same output: for all $q \in Q$, $\omega(q, a) = \omega(\delta(q, a), a)$. 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” $a, b \in \Sigma$, such that $\omega(q, a) \neq \omega(\delta(q, b), a)$, then the system exhibits complementarity: measuring b changes the state of the system from q to $q' = \delta(q, b)$, and as a consequence, we lose the ability to know $\omega(q, a)$. We thus cannot “measure” both a and b at the same time, which serves to show that complementarity itself is not incompatible with value definiteness.

3.3. 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; that is, using standard quantum measurements and other techniques to which we currently have access.

Let E be an experiment involving a quantum system, and let Λ_A be the set of parameters λ corresponding to the situation in which the value $v(A)$ of an observable A is known. We assume for simplicity that the observables A and B have discrete spectra (as for bounded systems), that is 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, is 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.

Formally, we say the set of extractors Ξ is restricted by complementarity if, for any two incompatible quantum observables A, B (i.e., $[A, B] \neq 0$), there does not exist an extractor $\xi \in \Xi$ and partially computable function f , such that, whenever the value $v(A)$ of the observable A is known, the following holds for an infinite set $\Lambda \subset \Lambda_A$: for all $\lambda \in \Lambda$, $f(\xi(\lambda)) = v(B)$, and $f(\xi(\lambda))$ is undefined for all $\lambda \in \Lambda_A \setminus \Lambda$.

It would be tempting to require that $v(B)$ cannot be “extracted” for any single trial $\lambda \in \Lambda_A$ without altering the system, but, as in the definition of predictability, we need to ensure that one cannot correctly obtain $v(B)$ simply by chance. Thus, this definition requires that the value $v(B)$ cannot be reliably extracted an infinite number of times. We stress that this does not imply that A and B cannot simultaneously have definite values, simply that we cannot know both at once.

Let us consider an experiment E_C 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 P_ϕ 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 this experiment is unpredictable relative to an agent whose predicting power is restricted by complementarity. More formally, if a set of extractors Ξ_C is restricted by complementarity, then the experiment E_C described above is unpredictable for Ξ_C . For otherwise, there would exist an extractor $\xi \in \Xi_C$ and a computable predictor P_{E_C} , such that, under any repetition procedure giving parameters $\lambda_1, \lambda_2, \dots$, we have $P_{E_C}(\xi(\lambda_i)) = x_i$ for infinitely many i and $P_{E_C}(\xi(\lambda_i))$ withheld otherwise, where x_i is the outcome of the i -th iteration/trial. However, if we define f , such that $f = P_{E_C}$ when prediction is not withheld and undefined otherwise, then the pair (ξ, f) contradicts the restriction by complementarity, and hence, E_C is unpredictable for Ξ_C .

It 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 restriction by complementarity, and hence, we gain little extra by considering this situation.

As a concrete example, consider the preparation of a spin- $\frac{1}{2}$ particle, for instance an electron, prepared in a $S_z = +\hbar/2$ state before measuring the complementary observable $2S_x/\hbar$ producing an outcome in $\{-1, +1\}$. 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 value definite) and is thus “contained” in the parameter λ . The assumption that Ξ_C is restricted by complementarity means that there is no extractor $\xi \in \Xi_C$ 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_C .

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 is, 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 functions, for example). This weaker notion of complementarity would thus seem insufficient to derive unpredictability for Ξ , although it would not show predictability either. We would thus, at least for the moment, be left unsure about the unpredictability of measurements limited by this weak notion of complementarity.

4. Unpredictability, Computability and Complementarity

Quantum randomness can be produced by measuring unpredictable quantum observables, and in an effort to understand more precisely the quality of this form of randomness, we showed in [21] that the result of repeatedly measuring a value-indefinite quantum observable always produces a strongly incomputable sequence of bits (technically, a bi-immune sequence, which means that no computable function can compute exactly the values of more than finitely many bits of the sequence). Since this type of incomputability represents a notion of purely algorithmic unpredictability [8], one may be tempted to think that this is a result not so much of quantum value indefiniteness, but rather of quantum unpredictability.

In [8], however, we showed that this is not the case: there are unpredictable experiments capable of producing both computable and strongly incomputable sequences when repeated *ad infinitum*. It is thus *a fortiori* also true for relativised unpredictability, and there is no immediate guarantee that measurements of complementary observables must lead to incomputable sequences, as is the case with value indefiniteness.

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 incomputability, much as value indefiniteness does.

Here, we show this not to be true in the strongest possible way. Specifically, we will show how the toy model of quantum systems we presented in Section 3.2.2 based on Mealy automata is unpredictable for predictors restricted by complementarity in a way analogous to that defined for quantum observables and, furthermore, that such systems can produce (low complexity) computable sequences when repeated.

Consider an experiment E_M involving the prediction of the outcome of a measurement on a (unknown, but fixed) Mealy automaton $M = (Q, \Sigma, \Theta, \delta, \omega)$, which we can idealise as a black box, with $\{x, z\} \in \Sigma$ characters in the input alphabet, output alphabet $\Theta = \{0, 1\}$ and satisfying the conditions that (1) for all $q \in Q$ and $a \in \Sigma$, $\omega(q, a) = \omega(\delta(q, a), a)$, and (2) x and z are complementary; that is, for all $q \in Q$ we have $\omega(q, z) \neq \omega(\delta(q, x), z)$ and $\omega(q, x) \neq \omega(\delta(q, z), x)$. Note that the specification of E_M does not require M to be in any particular initial state, which in general is unknown. This automaton is deliberately specified to resemble measurements on a qubit and can be viewed as a toy model of a two-dimensional value-definite quantum system, where the outcomes 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 [4], even if it is not intended to be particularly realistic. We complete the specification of E_M by considering a trial of E_M to be the output on the string xz , that is if the automaton is initially in the state q , the output is $\omega(\delta(q, x), z)$, and the final state is $\delta(\delta(q, x), z)$. This is a clear analogy to the preparation and measurement of a qubit using complementary observables, of the type discussed earlier.

Let Λ_x be the set of parameters λ corresponding to M being in a state q in the set $\{q \in Q \mid \delta(q', x) = q \text{ for some } q' \in Q\}$. Note that such a state q satisfies $\omega(q', x) = \omega(\delta(q', x), x) = \omega(q, x)$, and hence, q is an “eigenstate” of x . In analogy to the definition for quantum observables, we will say that a set Ξ_M of extractors is restricted by M -complementarity if there is no extractor $\xi \in \Xi_M$ and partially computable function f , such that, if M is in a state q with $\lambda \in \Lambda_x$, the following holds for an infinite set $\Lambda \subset \Lambda_x$: for all $\lambda \in \Lambda$, $f(\xi(\lambda)) = \omega(q, x)$, and $f(\xi(\lambda))$ is undefined for all $\lambda \in \Lambda_x \setminus \Lambda$.

Let us show that E_M is unpredictable for any set Ξ_M of extractors restricted by M -complementarity, the proof of which mirrors that of the unpredictability for quantum observables in Section 3.3. Let us assume for the sake of contradiction that E_M is predictable for Ξ_M : that is, there is a predictor P_{E_M} and an extractor $\xi \in \Xi_M$, such that E_M is predictable for ξ . Thus, from the definition of predictability, when E_M is repeated under any repetition procedure, P_{E_M} must provide infinitely correct predictions and no incorrect ones. This must thus be true if E_M is repeated by inputting x to prepare the i -th trial, so that each λ_i is in Λ_x . For such a repetition procedure, the output of the i -th trial of E_M is precisely $\omega(\delta(q_i, x), z) = \omega(q_i, z)$, and for each trial, we have either $P_{E_M}(\xi(\lambda_i)) = \omega(q_i, z)$ or prediction withheld. However, if we define f , such that $f = P_{E_M}$ when prediction is not withheld, and undefined otherwise, then the pair (ξ, f) contradicts the restriction by M -complementarity, and hence, we conclude that E_M is unpredictable for Ξ_M .

It is important to understand that the unpredictability of E_M for any Ξ_M restricted by M -complementarity expresses the inability to give a single predictor/extractor pair that gives correct predictions for any valid repetition procedure, rather than just for a single repetition procedure. Indeed, if we consider perhaps the simplest repetition procedure, where the final state of the system after the i -th trial is the initial state for the $(i + 1)$ -th trial, then the sequence produced by the infinite repetition of trials is necessarily computable, even cyclic, since it simply represents the run of the automaton. This computability, however, fails to provide a predictor for E_M , since it would fail to provide correct predictions for other repetition procedures, where, for example, a new copy of the system in a new initial state is used for each trial. This same observation means that the fact that any Mealy automaton is learnable in the infinite limit [34] equally fails to provide a general method of prediction for E_M .

This example does show, however, that the experiment E_M , although unpredictable for Ξ_M , is capable of producing computable sequences, even if it need not do so under all repetition procedures, and hence, computability is not excluded by complementarity.

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, such as $000\dots$, but it could equally be something far less obvious, such as the digits in the binary expansion of π at prime indices, that is $\pi_2\pi_3\pi_5\pi_7\pi_{11}\dots$. Hence, this scenario cannot be easily ruled out empirically, regardless of the

computability, that is the 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 [8,35,36]; such models need not contradict any principle of complementarity and can be computable or incomputable.

5. Summary

In this paper, following on from previous work in [8], we developed a revised and more nuanced formal model of (un)predictability for physical systems. By considering prediction agents with access to restricted sets of extractors with which to obtain information for prediction, this model allows various intermediate degrees of prediction to be formalised.

Although models of prediction such as this can be applied to arbitrary physical systems, we have discussed in detail their utility in helping to understand quantum unpredictability, which plays a key role in quantum information and cryptography.

We showed that, unlike measurements certified by value indefiniteness, those certified by complementarity alone are not necessarily simply unpredictable: they are unpredictable relative to the ability of the predicting agent to access the values of complementary observables, a more epistemic, relativised notion of predictability. This is a general result about complementarity, not specifically about quantum complementarity; in particular, one may aim to have certification by both complementarity and value indefiniteness. Indeed, in dimension three and higher Hilbert space, relative to the assumptions of the Kochen–Specker theorem [21], one has certification by both properties value indefiniteness, thus providing 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 that should not be forgotten [8]. 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.

The fact that quantum complementarity provides a weaker certification than value indefiniteness is emphasised by our final result, showing that complementarity is compatible with the production of computable sequences of bits, which is not true for value indefiniteness. Thus, 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 the Marie Curie FP7-PEOPLE-2010-IRSES-269151-RANPHYS grant. We thank the anonymous referees for useful comments.

Author Contributions

All authors contributed equally to the research and results in this paper. The initial draft was written by the first author, and all authors contributed to subsequent revisions. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Zeilinger, A. The message of the quantum. *Nature* **2005**, *438*, 743.
2. Fitzsimons, J.F.; Rieffel, E.G.; Scarani, V. Quantum frontier. In *Computation for Humanity: Information Technology to Advance Society*; Zander, J., Mosterman, P.J., Eds.; CRC Press: Boca Raton, FL, USA, 2013.
3. Stefanov, A.; Gisin, N.; Guinnard, O.; Guinnard, L.; Zbinden, H. Optical quantum random number generator. *J. Mod. Opt.* **2000**, *47*, 595–598.
4. Kochen, S.; Specker, E.P. The problem of hidden variables in quantum mechanics. *J. Math. Mech. (Now Indiana Univ. Math. J.)* **1967**, *17*, 59–87.
5. Bell, J.S. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **1966**, *38*, 447–452.
6. Berta, M.; Christandl, M.; Colbeck, R.; Renes, J.M.; Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **2010**, *6*, 659–662.
7. Dynes, J.F.; Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. A high speed, postprocessing free, quantum random number generator. *Appl. Phys. Lett.* **2008**, *93*, 031109.
8. Abbott, A.A.; Calude, C.S.; Svozil, K. On the unpredictability of individual quantum measurement outcomes. In *Fields of Logic and Computation II—Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday*; Beklemishev, L.D., Blass, A., Dershowitz, N., Finkbeiner, B., Schulte, W., Eds.; Springer: Cham, Switzerland, 2015; Volume 9300, pp. 69–86.
9. Popper, K.R. Indeterminism in quantum physics and in classical physics I. *Br. J. Philos. Sci.* **1950**, *1*, 117–133.
10. Wolpert, D.H. Physical limits of inference. *Phys. D* **2008**, *237*, 1257–1281.
11. Eagle, A. Randomness is unpredictability. *Br. J. Philos. Sci.* **2005**, *56*, 749–790.
12. Werndl, C. What are the new implications of chaos for unpredictability? *Br. J. Philos. Sci.* **2009**, *60*, 195–220.
13. Einstein, A.; Podolsky, B.; Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **1935**, *47*, 777–780.

14. Copeland, B.J. The Church-Turing Thesis. In *The Stanford Encyclopedia of Philosophy*, Fall 2008 ed.; Zalta, E.N., Ed.; The Metaphysics Research Lab, Stanford University: Stanford, CA, USA, 2008.
15. Longo, G.; Paul, T. The mathematics of computing between logic and physics. In *Computability in Context: Computation and Logic in the Real World*; Cooper, S., Sorbi, A., Eds.; Imperial College Press/World Scientific: London, UK, 2008; Chapter 7, pp. 243–274.
16. Paul, T. Semiclassical analysis and sensitivity to initial conditions. *Inf. Comput.* **2009**, *207*, 660–669.
17. Devaney, R.L. *An Introduction to Chaotic Dynamical Systems*, 2nd ed.; Addison-Wesley: Redwood, CA, USA, 1989.
18. Pironio, S.; Acín, A.; Massar, S.; Boyer de la Giroday, A.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; *et al.* Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024.
19. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
20. Zeilinger, A. A Foundational principle for quantum mechanics. *Found. Phys.* **1999**, *29*, 631–643.
21. Abbott, A.A.; Calude, C.S.; Conder, J.; Svozil, K. Strong Kochen–Specker theorem and incomputability of quantum randomness. *Phys. Rev. A* **2012**, *86*, 062109.
22. Abbott, A.A.; Calude, C.S.; Svozil, K. A variant of the Kochen–Specker theorem localising value indefiniteness. *J. Math. Phys.* **2015**, *56*, 102201.
23. Pitowsky, I. Infinite and finite Gleason's theorems and the logic of indeterminacy. *J. Math. Phys.* **1998**, *39*, 218–228.
24. Fritz, T. Nonlocality with less complementarity. *Phys. Rev. A* **2012**, *85*, 022102.
25. Wright, R. Generalized urn models. *Found. Phys.* **1990**, *20*, 881–903.
26. Svozil, K. Logical equivalence between generalized urn models and finite automata. *Int. J. Theor. Phys.* **2005**, *44*, 745–754.
27. Pauli, W. Die allgemeinen Prinzipien der Wellenmechanik. In *Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I*; Flüge, S., Ed.; Springer: Berlin, Germany, 1958; pp. 1–168. (in German)
28. Heisenberg, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **1927**, *43*, 172–198. (in German)
29. Busch, P.; Lahti, P.; Werner, R.F. Measurement uncertainty relations. *J. Math. Phys.* **2014**, *55*, 042111.
30. Cowen, R. Proof mooted for quantum uncertainty. *Nat. News* **2013**, *498*, 419–420.
31. Rozema, L.A.; Darabi, A.; Mahler, D.H.; Hayat, A.; Soudagar, Y.; Steinberg, A.M. Violation of Heisenberg's measurement-disturbance relationship by weak measurements. *Phys. Rev. Lett.* **2012**, *109*, 100404.
32. Robertson, H.P. The uncertainty principle. *Phys. Rev.* **1929**, *34*, 163–164.
33. Popper, K.R. *Quantum Theory and the Schism in Physics*; Routledge: London, UK, 1992.
34. Gold, E.M. Limiting recursion. *J. Symb. Log.* **1965**, *30*, 28–48.

35. Bohm, D. A suggested interpretation of the quantum theory in terms of “hidden” variables. I. *Phys. Rev.* **1952**, *85*, 166–179.
36. Bohm, D. A suggested interpretation of the quantum theory in terms of “hidden” variables. II. *Phys. Rev.* **1952**, *85*, 180–193.

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).