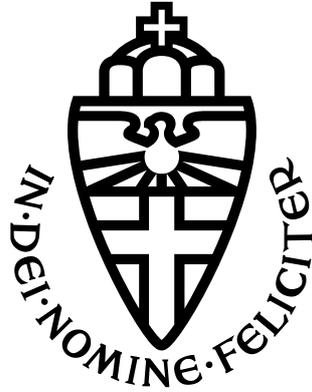


RADBOUD UNIVERSITY NIJMEGEN



FACULTY OF SCIENCE

An algorithmic perspective on randomness in quantum mechanics

THESIS BSC MATHEMATICS

Author:
Jonas KAMMINGA

Supervisor:
Prof. dr. Klaas LANDSMAN

Second reader:
dr. Sebastiaan TERWIJN

June 2019

Abstract

This thesis investigates the precise kind of randomness generated by quantum measurements. First a rigorous definition of randomness is given using the theory of algorithmic randomness. Thereafter it is investigated if there are quantum measurements of which it can be shown that they can be used to generate random finite or infinite binary strings. First, no go theorems from quantum theory are discussed. Second, articles attempting to answer this are studied. Third, the justifications given by a manufacturer of quantum random number generators are reviewed. Finally, this thesis considers an experimental method for validating the randomness of quantum measurements.

Contents

1	Introduction	3
2	Preliminaries	4
2.1	The space of infinite binary sequences	4
2.2	Turing machines and the halting problem	5
2.3	Computability and computable enumerability	5
2.3.1	Complexity of reals and real valued functions	6
2.4	Martingales	6
2.5	The quantum mechanical formalism	7
3	Algorithmic randomness	9
3.1	Paradigm 1: the incompressibility paradigm	10
3.1.1	Prefix free complexity	11
3.1.2	Prefix-free randomness	12
3.2	Paradigm 2: the measure theoretic paradigm	13
3.3	Paradigm 3: the unpredictability paradigm	14
3.4	Other notions of randomness	14
4	Algorithmic randomness of the results of quantum mechanics	15
4.1	No go theorems in quantum mechanics	16
4.1.1	The Kochen Specker theorem	17
4.1.2	The free will theorem	17
4.1.3	Bell inequalities	19
4.2	Previous results about the algorithmic randomness of quantum mechanics	20
4.2.1	Senno's thesis	21
4.2.2	Yurtsever's article	22
4.2.3	Calude & Svozil	23

4.2.4 Rogers	24
5 Randomness of quantum random number generators	25
5.1 ID quantique's <i>quantis</i>	25
5.2 Random numbers certified by Bell's theorem	26
6 Conclusion	27

1 Introduction

Randomness has become of vital importance to our modern style of living. We use it for our entertainment, for example in the casino or in computer games. We use encryption software based on randomness every time we send a WhatsApp text, receive an email or manage your finances online. Since randomness has become so important, there are two questions we might ask ourselves: what exactly are random numbers and how can we generate them?

Defining randomness is not exactly an easy task. When we have a finite binary string consisting of only ones, it feels less random than a string such as 001010001110010011, generated by throwing a coin. However, the probability of generating each string is exactly the same, namely 2^{-n} , where n is the length of the string. The mathematical theory of algorithmic randomness is concerned with defining randomness in a manner consistent with both our intuition and probability theory. In this thesis we will look at the definition of randomness given by this field of mathematics and apply it to quantum mechanics.

Probably the best known example of a randomness generator is a coin flip. Like other methods such as a roulette wheel, a coin flip generates randomness because it is a (classical) system that is very sensitive to the initial conditions and is therefore hard to predict. However, the coin flip is not perfectly random. A coin being flipped behaves exactly according to Newtonian mechanics. Therefore it is, in principle, possible to perfectly predict the outcome of the coin toss. In practice this is very difficult, but it has been shown that there are ways to slightly influence the statistics of a coin flip [6]. Furthermore, it is very difficult to generate the huge amount of random numbers that are required for encryption using a coin.

One other method of generating random numbers is actually not a method of generating random numbers at all. For many purposes so called pseudo-random numbers are used. These are numbers generated by pieces of software or algorithms called pseudo-random number generators (pseudo-RNGs). While pseudo-RNGs are designed to produce numbers which resemble random numbers as well as possible, they are ultimately deterministic computer programs. Therefore, their output can be perfectly predicted by reverse-engineering the algorithm. This makes them a risk factor when used for the encryption of sensitive information. This is expressed by von Neumann's famous quote: "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin." [19] In an effort to make pseudo-RNGs less vulnerable against reverse engineering opponents, some of them take system data such as the time of the day or fluctuations in cursor movement as an input and generate randomness from them. However, this does still not guarantee the complete safety of the encrypted data. One example of this is a security flaw found in a Netscape protocol in 1995. Two students reverse engineered the code and discovered it was based on the clock of the system which was relatively easy to guess. This allowed them to reduce the time necessary to break into the protocol to mere minutes. [17]

One recent method for generating random numbers is to use quantum measurements. The physical theory of quantum mechanics is often said to be fundamentally random. One advantage quantum generated randomness would have over randomness

generated by classical physical systems is that it is easier to perform a large number of quantum measurements in a short time than it is to throw a similar number of coins in a short time. Additionally, since quantum measurements are fundamentally indeterministic, it does not suffer from the problem classical systems have that complete knowledge would allow for perfect predictions. This is also an advantage quantum-generated randomness has over computer generated randomness. For these reasons, commercial companies have tried to make systems that can quickly perform quantum measurements in order to generate randomness from these. Systems like this are known as quantum random number generators (QRNGs).

But how can we guarantee that numbers generated by these QRNGs are actually random? One example of a system that is not deterministic but also certainly not random is a box that for every even output gives a 1 and for every odd output flips a coin and outputs the result. Clearly, quantum mechanics being indeterministic is by itself not enough to guarantee randomness.

In this thesis we will first give a mathematically precise definition of randomness. We will then look at results from quantum theory showing its fundamental indeterministic behaviour. After that, we will turn our attention to attempts to prove that the outcomes of certain quantum measurements must be random. We will also look at justifications given by a manufacturer of quantum random number generators that their devices output random numbers. Finally, we will look at a method to experimentally verify the randomness of quantum random number generator outputs.

2 Preliminaries

This section gives a very brief overview of the preliminary knowledge required to understand algorithmic randomness and quantum mechanics. The part about quantum mechanics is mostly based on Foundations of Quantum Theory by Klaas Landsman [13, ch. 2]. For the other parts I have based myself on Algorithmic Randomness and Complexity by Rodney Downey and Denis Hirschfeldt [7, ch. 1-7], an Introduction to Kolmogorov Complexity and its Applications by Ming Li and Paul Vitányi [16] and Calibrating Randomness by Rodney Downey, Denis Hirschfeldt, André Nies and Sebastiaan Terwijn [8].

2.1 The space of infinite binary sequences

The field of algorithmic randomness defines and studies the randomness of elements of the so called Cantor space 2^ω . Elements $X \in 2^\omega$ are often associated with the set

$$X = \{n : X(n) = 1\}$$

and are thus sometimes referred to as sets in the literature. The Cantor space is endowed with the tree topology with basic clopens $[\sigma] := \{X \in 2^\omega : \sigma \prec X\}$, where σ is a finite binary string. The symbol \prec denotes that σ is a prefix of X , so $[\sigma]$ contains all infinite binary strings that have σ as a prefix.

We can define the uniform Lebesgue measure on 2^ω by defining the measure of any basic clopen set as $\mu([\sigma]) := 2^{-|\sigma|}$, where $|\sigma|$ denotes the length of σ . It turns out that the Cantor space with this measure is measure-theoretically isomorphic to the interval $[0, 1]$ which is why elements $X \in 2^\omega$ are sometimes referred to as reals. In short, there are three names for elements $X \in 2^\omega$: infinite binary strings, sets and reals. In order to avoid confusion with other sets or other reals I will refer to elements of the Cantor space as infinite binary strings.

We will also review randomness of finite binary strings. The set of all finite binary strings is written as $2^{<\omega}$. For any $\sigma \in 2^{<\omega}$ and $\tau \in 2^{<\omega}$ we write $|\sigma|$ for the length of σ and $\sigma\tau$ for the concatenation of τ and σ . For any infinite binary string $X \in 2^\omega$ we write $X \upharpoonright n$ for the finite binary string obtained by taking only the first n digits of X .

2.2 Turing machines and the halting problem

Turing machines were first introduced by Alan Turing, who called them automatic machines [30]. The exact definition of a Turing machine is too involved to go into here, but they are easy to understand intuitively as a computer executing a given program. A Turing machine takes a natural number, or, equivalently, a finite binary string as an input and starts computing. It then either finishes running and gives an output. We call this halting. A Turing machine can also not stop and keep running forever, in which case we say it does not halt. We write $T(\sigma) \downarrow$ if Turing machine T with input σ halts and write $T(\sigma) \uparrow$ if it does not halt. The famous unsolvability of the halting problem states that no algorithm exists that for every Turing machine with any input determines if it halts or not.

For any finite binary string $\sigma \in 2^{<\omega}$ we write $T(\sigma)$ for the output of the Turing machine T with this input (think of a computer executing some algorithm with input σ). A Turing machine U is called **universal** if it can simulate any other Turing machines. That is, for any Turing machine T there exist a $\rho \in 2^{<\omega}$ such that for any $\sigma \in 2^{<\omega}$ we have $T(\sigma) = U(\rho\sigma)$.

2.3 Computability and computable enumerability

The theory of algorithmic randomness is based on the notions of computability and computable enumerability. We say a partial function $f : 2^{<\omega} \rightarrow 2^{<\omega}$ is **partial computable** if there exists a Turing machine T such that for every $\sigma \in \text{dom}(f)$ we have $T(\sigma) \downarrow$ and $T(\sigma) = f(\sigma)$. We also require that for all $\sigma \notin \text{dom}(f)$ we have $T(\sigma) \uparrow$. If f is total, that is, if $\text{dom}(f) = 2^{<\omega}$, we simply say that f is computable. A family of functions f_0, f_1, \dots is called **uniformly (partial) computable** if there is a (partial) computable function f such that $f(n, x) = f_n(x)$ for all n and x .

We can also put a time bound on the computability of f . If we have a time function $T : \mathbb{N} \rightarrow \mathbb{N}$ we say that f is **computable in $O(T(n))$ -time** if there exists a Turing machine M computing f and a constant c such that for almost all $\sigma \in 2^{<\omega}$, M computes σ within $c \cdot T(|\sigma|)$ time steps.

A subset $A \subseteq 2^{<\omega}$ is called **computably enumerable**, often abbreviated as **c.e.**, if it is the domain of some partial computable function. Equivalently, a subset $A \subseteq 2^{<\omega}$ is com-

putably enumerable iff either $A = \emptyset$ or there exists a (total) computable function f from $2^{<\omega}$ onto A . If A is infinite this function can be chosen to be injective. A collection of sets A_0, A_1, \dots is called **uniformly computably enumerable** if each $A_n = \text{dom}(f_n)$ for a collection f_0, f_1, \dots of uniformly partial computable functions. Computably enumerable sets are often called Σ_1^0 sets. If both A and $2^{<\omega} \setminus A$ are computably enumerable we say that A is **computable**. Similarly, if both A_0, A_1, \dots and their complements are uniformly c.e. we say that they are **uniformly computable**. Intuitively, you can think about a computably enumerable set as being a set of which we can enumerate all elements that are in the set, but of which we cannot necessarily enumerate all the elements that are not in the set. If we can also enumerate all elements not in the set, it is a computable set.

Example 1. Probably the most famous example of a set that is computably enumerable but not computable is diagonal the halting set $K = \{T_n : T_n(n) \downarrow\}$, i.e. the set of all Turing machines in some enumeration of Turing machines such that the n -th machine halts on input n . It can be proven that this set is not computable. In fact, this can be used to prove the uncomputability of the halting problem. However, we can make an enumeration of K by first enumerating all Turing machines T_n that halt on n in 1 time step, then all Turing machines that halt in 2 timesteps and so on. But since the set is not computable we cannot make an enumeration of the complement of K .

2.3.1 Complexity of reals and real valued functions

One can also define the complexity of real numbers, and even real valued functions. As we will need notions of complexity for real valued functions later we will discuss these here. For each real α we can define the **left cut** of α as $L(\alpha) = \{q \in \mathbb{Q} : q < \alpha\}$. These left cuts can be used to uniquely identify each real. We can now define a real α to be **computable** if $L(\alpha)$ is computable. If $L(\alpha)$ is c.e. we define α to be **left computably enumerable (left-c.e.)**. For a function $f : D \rightarrow \mathbb{R}$ we say it is **computably enumerable (c.e.)** if the set $\{(x, q) \in D \times \mathbb{Q} : q < f(x)\}$ is computably enumerable. If this set is computable, then we say f is **computable**.

2.4 Martingales

One tool that will be important for the discussion of randomness of infinite binary strings is the martingale. A **martingale** is a function $d : 2^{<\omega} \rightarrow \mathbb{R}_{\geq 0}$ with the property that for every $\sigma \in 2^{<\omega}$ we have

$$d(\sigma) = \frac{1}{2} \left(d(\sigma 0) + d(\sigma 1) \right). \quad (1)$$

This property is known as the **averaging condition**. We call d a **supermartingale** by relaxing the equality to a \geq sign. One intuitive way to think about a martingale is as a betting strategy. We start with a certain amount of money and at every step we bet some part of our money on the next digit of the infinite sequence being a one and the rest on it being a zero. The money we bet on the correct digit is doubled and the rest is lost. The outcome $d(\sigma)$ of a martingale is the amount of money we have after applying the betting strategy corresponding to d and the outcomes having been σ .

We say that a (super)martingale *succeeds* on an infinite binary sequence $X \in 2^\omega$ if

$$\limsup_{n \rightarrow \infty} d(X \upharpoonright n) = \infty. \quad (2)$$

Formulated using our betting analogy: a martingale succeeds on an infinite binary sequence X if the betting strategy corresponding to it will allow us to make arbitrary amounts of money when betting on the digits of X . We require arbitrary amounts of money for our notion of success because we want the strategy to consistently and correctly predict digits of X . The set of all $X \in 2^\omega$ on which a martingale d succeeds is denoted by S_d .

Example 2. To illustrate the relation between betting strategies and martingales consider the following scenario: We are in a casino playing a game of betting on the digits of a binary string. At every stage we divide our capital betting a certain portion of it on the next digit being a 1 and the rest on the next digit being a 0. The amount of money we bet on the digit that shows up is doubled and the rest is lost.

We have devised the strategy of, at every stage, betting 70% of our capital on the next digit being a 1 and 30% on the next digit being a 0. Suppose we start out with a capital of 1\$. Following our strategy, we bet 0.7\$ on the first digit being a 1 and 0.3\$ on the first digit being a 0. If the first digit turns out to be a 1, we will have 1.4\$ after the first stage, but if the first digit is a 0 we will only have 0.6\$. The money we have after a certain string has been revealed is exactly the value of the martingale of that string. So in this case $d(1) = 1.4$ and $d(0) = 0.6$. Continuing we get that $d(11) = 1.4 \cdot 0.7 \cdot 2 = 1.96$ and $d(110) = 1.96 \cdot 0.3 \cdot 2 = 1.176$. It is clear that this betting strategy can make an infinite amount of money if the string we are betting on ends in infinitely many ones. Therefore this martingale succeeds on such strings.

The following important theorem by Ville [31] relates the concept of martingales with measure theory:

Theorem 1. (Ville 1939 [31]) *For any subset $\mathcal{A} \subseteq 2^\omega$ the following two statements are equivalent:*

1. \mathcal{A} has Lebesgue measure 0;
2. There exists a martingale d such that $\mathcal{A} \subseteq S_d$.

2.5 The quantum mechanical formalism

The quantum-mechanical formalism models the *state space* of a physical system as a Hilbert space \mathcal{H} (a complex vector space with an inner product denoted by $\langle \cdot, \cdot \rangle$). For our purposes it is enough to consider finite dimensional Hilbert spaces, so we restrict our attention to those. The state of the system is described by a unit vectors of this Hilbert space but it can also be a statistical mixture of unit vectors. These correspond to density operators. A *density operator* ρ is a positive operator on \mathcal{H} with $\text{Tr}(\rho) = 1$. (Being a positive operator means that $\langle \rho\psi, \psi \rangle \geq 0$ for all $\psi \in \mathcal{H}$.) Here $\text{Tr}()$ denotes the trace function which is unproblematic for operators on a finite dimensional Hilbert space.

In the formalism of quantum mechanics, the probabilities to obtain measurement outcomes are described by the *Born rule*. This rule is single-handedly responsible for all

predictions made by quantum mechanics. Quantum mechanical observables are represented by self-adjoint operators on the Hilbert space \mathcal{H} . The spectrum of a self-adjoint operator a is defined as the set of all eigenvalues of a (since we only consider finite dimensional Hilbert spaces) and is denoted as $\sigma(a)$. We can make a spectral decomposition of each self-adjoint operator $a = \sum_{\lambda \in \sigma(a)} \lambda \Pi_\lambda$ where Π_λ is the projection onto the eigenspace corresponding with eigenvalue λ . According to the Born rule, the probability that, upon measurement of a on a state described by a density operator ρ , we obtain the value λ is given by: $p_a(\lambda) = \text{Tr}(\Pi_\lambda \rho)$. If we assume that $\rho = |\psi\rangle\langle\psi|$ (this is Dirac's "bra-ket" notation where $|\psi\rangle\langle\phi|\chi = \langle\phi, \chi\rangle\psi$) and that $\lambda \in \sigma(a)$ is non-degenerate we obtain the perhaps better known form of the Born rule: $P_a^\Psi(\lambda) = |\langle\Psi, \nu_\lambda\rangle|^2$, where ν_λ is the eigenvector corresponding to the eigenvalue λ , that is $a\nu_\lambda = \lambda\nu_\lambda$.

In quantum theory measuring a state often changes that state. It tells us that if we perform a measurement and obtain a value λ , the state ρ changes to $\rho' = \frac{1}{\text{Tr}(\Pi_\lambda \rho)} \Pi_\lambda \rho \Pi_\lambda$.

You can think about performing a measurement of a on a particle as asking the particle in which of the eigenspaces of a it is. For each orthonormal basis $\mathbb{B} = \{|0\rangle, \dots, |n-1\rangle\}$ of H we can define an operator $A_{\mathbb{B}} = \sum_{i=0}^{n-1} a_i |i\rangle\langle i|$ with all the a_i different. The eigenspaces of this observable will each be the span of a single basis vector. If we measure this observable we say that we measure with respect to the basis \mathbb{B} .

One system we will look at is the **qubit**. The qubit is the simplest non-trivial quantum system and has Hilbert space \mathbb{C}^2 . One physical example of a qubit is the spin of an electron. The standard basis on \mathbb{C}^2 is denoted by $\{|0\rangle, |1\rangle\}$. However, we can also define another basis $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. Using these bases we can define the Pauli observables which will be important for our purposes. They are given in matrix form and spectral decomposition as:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle+| - |-\rangle\langle-| \quad (3)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (4)$$

According to the Born rule described above, when we prepare the spin of an electron in the $|-\rangle$ state and perform a measurement of σ_z we will either obtain $+1$ or -1 , both with probability $\frac{1}{2}$. If we obtain $+1$, the particle will be in the $|0\rangle$ state after the measurement and if we measure -1 it will be in the $|1\rangle$ state. We will be looking at a situation where we keep repeating these measurements to generate a binary string and then look at what we can say about the randomness of this string using the theory of algorithmic randomness.

One important feature unique to quantum theory is **entanglement**. Essentially, we say that two systems are entangled if they cannot be described independently of each other. If we have two systems with Hilbert spaces \mathcal{H}_A and \mathcal{H}_B , then the composite system is described by the tensor product of these two Hilbert spaces $\mathcal{H}_A \otimes \mathcal{H}_B$. We will often write $|vw\rangle$ instead of $|v\rangle \otimes |w\rangle$. There are many vectors in $\mathcal{H}_A \otimes \mathcal{H}_B$ that cannot be expressed as $v_A \otimes v_B$ for some $v_A \in \mathcal{H}_A$ and $v_B \in \mathcal{H}_B$. One example of this is $(|10\rangle - |01\rangle)/\sqrt{2} \in \mathbb{C}^2 \otimes \mathbb{C}^2$. If a state in a composite system cannot be described as the tensor product of two vectors, we say that the subsystems are **entangled**.

One other system we will look at is a system made up of two qubits in an entangled state $(|1_A 0_B\rangle - |0_A 1_B\rangle)/\sqrt{2} \in \mathbb{C}^2 \otimes \mathbb{C}^2$. Suppose that Alice and Bob both have access to

one of these entangled qubits and that both perform a measurement of σ_z . Quantum theory tells us that Alice will obtain value -1 with probability $\frac{1}{2}$ and that the system will then be in the $|1_A 0_B\rangle$ state. Also with probability $\frac{1}{2}$, she will measure $+1$ and the system will be in the $|0_A 1_B\rangle$ state. Let us assume that she measures $+1$. Since the system is now in the $|0_A 1_B\rangle$ state Bob is required to measure -1 . Similarly, if Alice obtains the value -1 , Bob will necessarily get the value $+1$. This correlation holds regardless of the distance separating Alice and Bob. However, since Bob is not able to determine if he measured -1 because the probabilities turned out that way or because Alice performed a measurement and measured $+1$ this correlation cannot be used for faster than light communication.

3 Algorithmic randomness

While everybody has an idea of what randomness means, it is not easy to define randomness rigorously. One attempt you might make at defining randomness is to define something as random if it is not the result of a deterministic process. However, this runs into problems. Suppose we generate an infinite binary string which is not a result of a deterministic process and then program a computer to output the digits of this string. Then the outputs of this computer are deterministic in the sense that if we look at the code, we know exactly what the computer will output next. But now the string is both random because we generated it without it being the result of a deterministic process and not random because it is also generated deterministically by the computer we programmed to do so. This would mean the randomness of a binary string is dependent on the process that generated it, but we would like to say something about its randomness independently of the process that generated it. Furthermore, if we have a string that was not generated by a deterministic process, we can dilute it by adding 1 at every even position. The resulting string still is not the result of a deterministic process, but is not random either.

One other attempt at defining randomness is the more statistical approach of defining an infinite binary string as random if it contains as many zeroes as ones. This is known as the law of large numbers. We can extend this by requiring all n -bit fragments to occur with their expected frequency 2^{-n} . This property is called normal. It is a good start to require this from random numbers. However, it is not enough as that would mean that Champernowne's number $C = 0100011011000001\dots$ is also random. Champernowne's number is generated by first concatenating all possible 1-bit fragments, then all 2-bit fragments and so on. One might feel that since there is such a clear and short way to describe the process of generating the string it should not be random.

Clearly, defining randomness is not a trivial task. The mathematical theory of algorithmic randomness uses tools and concepts from computability theory to define randomness. Within the field there are several paradigms one can use to come to a definition of randomness. We will look at the main three paradigms, which all arrive at the same definition of randomness, called 1-randomness. We will then proceed by considering some other weaker notions of randomness. Defining randomness using these three paradigms was first done in *Calibrating Randomness* by Rodney Downey, Denis

Hirschfeldt, André Nies and Sebastiaan Terwijn [8]. I will follow this article closely in the following section.

3.1 Paradigm 1: the incompressibility paradigm

The first paradigm for defining randomness states that a random string should be incompressible: it should be impossible to give a description of the string that is significantly shorter than the string itself. To formalise this idea we introduce *Kolmogorov complexity*. We will first apply this concept to finite binary strings and then extend it to infinite binary strings.

Example 3. To understand the concept behind Kolmogorov complexity, let us consider the following three finite binary strings:

1. 101010101010101010101010101010
2. 110010010000111111011010101000
3. 100001101100111101001011111011

Obviously, the first string should not be called random since it is simply 10 repeated 15 times. The second string might look random on first sight but actually is the first 30 digits of π in binary and should therefore not be called random either. The third string, however, was generated by flipping a coin 30 times. We should therefore at least expect the third string to be random. One way to formalise this intuition is to use the idea of Kolmogorov complexity. Both the first and the second strings can be described in a shorter way as "10 repeated 15 times" and "first 30 binary digits of π " respectively. Of course, for these short strings, the difference between the length of the description and the length of the string itself is quite small. However, the description of 10 repeated 500000 times or the first one million digits of π is significantly shorter than the strings themselves. For the third string there is no short description. Therefore we can call the third string random.

Given a fixed universal Turing machine U , the *plain Kolmogorov complexity* of a finite binary string $\sigma \in 2^{<\omega}$ is defined to be:

$$C(\sigma) = \min\{|\tau| : U(\tau) = \sigma\}$$

Note that a different choice for the universal Turing machine will result in a different plain Kolmogorov complexity. However, since the machines are universal and can therefore imitate each other, the difference will only be a fixed constant.

We can now define $\sigma \in 2^{<\omega}$ to be *Kolmogorov k -random*, where $k \in \mathbb{N}$, if $C(\sigma) \geq |\sigma| - k$. We will often leave the constant unspecified and simply talk about Kolmogorov randomness.

One property of Kolmogorov randomness, which can be seen as a weakness, is that we can only prove the Kolmogorov randomness of finitely many finite binary strings, although infinitely many are in fact random. This follows from the immunity of the set of Kolmogorov random strings, which was shown by Barzdin[1]. *Immunity* means that there is no infinite c.e. subset of the set of Kolmogorov random strings. To see that the set

of Kolmogorov random strings is immune, we assume that there does exist a c.e. subset and derive a contradiction. If there exists a c.e. subset, then there exists an injective computable function $\psi : \mathbb{N} \rightarrow 2^{<\omega}$ such that $\psi(n)$ is Kolmogorov random for all n . We can now obtain a sequence $\phi(0), \phi(1), \phi(2), \dots$ such that there are infinitely many $m \in \mathbb{N}$ with $|\phi(m)| \geq m$ and hence $C(\phi(m)) \geq m$. Clearly, ψ and m together give a description of $\psi(m)$ and therefore $C(\psi(m)) \leq \log(m) + k$ for some constant k independent of m . We now have $m \leq C(\phi(m)) \leq \log(m) + k$ for infinitely many m . But this can only be true for finitely many m so we obtain a contradiction and conclude that the set of Kolmogorov random strings is indeed immune.

It is possible to enumerate all possible proofs and check if they proof that some string is Kolmogorov random. Because of this, if there were infinitely many strings that are provably Kolmogorov random, we could enumerate infinitely many Kolmogorov random strings. We have just seen that this is impossible, so it cannot be possible to prove Kolmogorov randomness of infinitely many strings.

3.1.1 Prefix free complexity

An issue with plain Kolmogorov complexity is that it does not extend to infinite strings. One would like to call an infinite string X random if and only if there exists a constant k such that every finite prefix of X is k -random. However, Martin-Löf showed that infinite strings with this property do not exist.

Theorem 2. (Martin-Löf 1966, see also Downey Hirschfeldt[7, p 113].) *For any constant k , if μ is a binary string of sufficient length, then there exists a initial segment σ of μ with $C(\sigma) < |\sigma| - k$.*

Proof. Consider an initial segment v of μ . Choose n such that v is the n th string of $2^{<\omega}$ under some ordering, for example the length-lexicographic ordering. Let ρ be the next n digits of μ after v and let $\sigma = v\rho$. To describe σ we only need ρ since the length of ρ combined with the ordering gives us v . Therefore, $C(\sigma) \leq |\rho| + c$ for some constant c . This c is independent of ρ or v because it only describes the process of taking the string corresponding to the length of the input from the ordering. We also have $|\sigma| = |v| + |\rho|$. If we now choose $|v| > c + k$ we have $C(\sigma) < |\sigma| - k$. \square

Martin-Löf's proofs works because not just the bits, but also the length of ρ encodes information. To fix the issue that the length of the input string encodes additional information, Chaitin and Levin [15][14][3] introduced a new measure of complexity that only takes the bits of a string into account and not the length. This new measure is called the prefix-free complexity K . To understand it, we first need to introduce the notions of prefix-free sets and prefix free Turing machines. We define a set of finite binary strings X to be **prefix-free** if for all $\sigma \in X$ and $\tau \in X$ with $\sigma \neq \tau$, σ is not a prefix of τ and τ is not a prefix of σ . A Turing machine T is prefix-free or a **prefix machine** if its domain is prefix-free. Usually, these machines are considered to be **self delimiting**. This means that the read head can only move one way. The machine is forced to accept strings without knowing if there are any more bits on the input tape. This automatically makes the domain prefix-free.

Analogously to a universal Turing machine, a **universal prefix** machine can be constructed by enumerating all prefix machines T_1, T_2, T_3, \dots and then defining $U(1^n\sigma) = T_n(\sigma)$. This U is clearly universal and prefix-free.

Definition 1. Let x be a finite binary string. The prefix-free complexity of σ is defined to be $K(\sigma) = \min\{|\tau| : U(\tau) = \sigma\}$, where U is a universal prefix machine.

Using the notion of a universal prefix machine we can define **Chaitin's Omega**[3] as

$$\Omega_U = \sum_{\sigma:U(\sigma)\downarrow} 2^{-|\sigma|}.$$

This number is also sometimes referred to as the **halting probability** of U . It can be proven that Ω_U is an example of a 1-random infinite binary string [3]. Also, it turns out that if one has access to the first n digits of Ω_U that one can then solve the halting problem for all inputs shorter than n on Turing machine U [16].

3.1.2 Prefix-free randomness

Using this definition we can give an improved notion of randomness. The notion follows what we did with Kolmogorov randomness by defining a string $\sigma \in 2^{<\omega}$ to be prefix-free random if $K(\sigma) \geq |\sigma|$. We relax this definition by a constant d and obtain the following definition:

Definition 2. A finite binary string $\sigma \in 2^\omega$ is prefix free d -random if $K(\sigma) \geq |\sigma| - d$.

Theorem 3. (Barzdin 1968 [1]) *The set of K -random finite strings is immune i.e. it has no c.e. subset.*

A consequence of this theorem is that there exists an upper bound such that strings longer than that bound cannot be proven to be K -random although most, in fact, are.

Proof. This proof is analogous to the result we have seen before by Barzdin that the set of Kolmogorov random strings is immune. Suppose that $\{\sigma : K(\sigma) \geq |\sigma| - d\}$ is not immune. Then it has a c.e. subset. Therefore we can find a computable injective function $\phi : \mathbb{N} \rightarrow \{\sigma : K(\sigma) \geq |\sigma| - d\}$ such that $|\phi(n)| \geq n$. Because ϕ and n together give a description of $\phi(n)$, we have $K(\phi(n)) \leq K(n) + O(1) \leq 2 \log(n) + O(1)$. But now we have $n - d \leq |\phi(n)| - d \leq K(\phi(n)) \leq 2 \log(n) + O(1)$, which can only hold for finitely many n . This contradicts our assumption. Therefore, $\{\sigma : K(\sigma) \geq |\sigma| - d\}$ is indeed immune. \square

Using the notion of K -randomness we can do what we could not do with the plain Kolmogorov complexity and give a randomness for infinite strings. With the plain complexity we ran into the problem that the length of the string could be used to encode additional information. In the prefix free case we do not run into the problem because the length of the string does not give additional information. This is because the domain is prefix free. After the machine has read and accepted the string σ there can be no more digits succeeding σ . The length of the input is known since σ is the only string starting with σ in the domain of the machine.

Definition 3. An infinite binary string X is called **Levin-Chaitin random** if there exists a constant c such that for every natural number n $K(X \upharpoonright n) \geq n - c$

3.2 Paradigm 2: the measure theoretic paradigm

The second paradigm we will consider is the *measure-theoretic* paradigm. It states that a random infinite binary string should have certain statistical properties. For example, we expect a random string to have approximately as many 0's as 1's and a 0 should be followed by a 1 about as often as it is followed by a 0. It was noted by Von Mises [18] that when considering a countable collection of statistical tests, a nonempty definition of randomness for reals exists. It was Church who later suggested that one should look at the collection of computable statistical tests. Martin-Löf noted that these statistical tests are special cases of measure 0 sets on the space of infinite binary strings 2^ω and stated that random infinite binary strings should be those that are not elements of effective (meaning c.e.) measure 0 subsets of 2^ω [20]. This idea gives us the following definition:

Definition 4. (Martin-Löf [20]) A collection of infinite binary strings \mathcal{A} is called Martin-Löf null (or Σ_1^0 -null) if there exists a uniformly c.e. sequence $\{U_n\}_{n \in \omega}$ of Σ_1^0 subsets $U_n \subseteq 2^\omega$ with $\mu(U_n) \leq 2^{-n}$ and $\mathcal{A} \subseteq \bigcap_n U_n$. Such a sequence $\{U_n\}_{n \in \omega}$ is called a Martin-Löf test. An infinite binary string $X \in 2^\omega$ is called **1-random** if $\{X\}$ is not Martin-Löf null.

This definition gives the same notion of randomness as the definition by Levin and Chaitin above. This was proven by Schnorr [27].

Theorem 4. Schnorr 1973 [27] *An infinite binary string $X \in 2^\omega$ is 1-random if and only if it is Levin Chaitin random.*

The proof is too lengthy to go into here but can be found in the book Algorithmic Randomness and Complexity by Downey and Hirschfeldt [7, p 232, 233]. From this point on I will refer to this notion of randomness as 1-randomness. Note that this is not the same as the previously introduced Kolmogorov k-randomness.

One interesting feature of Martin-Löf randomness is that there exists a universal Martin-Löf test. This is a test $\{U_n\}_{n \in \omega}$ such that an infinite binary string X is Martin-Löf random if and only if $X \notin \bigcap_n U_n$. To define such a universal test, consider a computable enumeration of all Martin-Löf tests $\{V_i^m\}_{m, i \in \omega}$ where $\{V_i^m\}_{i \in \omega}$ denotes the m -th test. By defining $U_n = \bigcup_k V_{k+n+1}^k$ we obtain a universal test since measures are countably additive. [20]

To motivate Martin-Löf's idea to consider statistical tests as measure 0 sets let us consider the following example which is due to Downey and Hirschfeldt [7, p 231]:

Example 4. Consider the subset $C \subseteq 2^\omega$ of all infinite binary sequences X such that for all $k \in \mathbb{N}$ we have that $X(2^k) = 0$. These infinite binary strings are clearly not random. If we are given an infinite binary string Y we can test its membership C within a confidence level of 2^{-n} by checking if for all $k < n$ we have $Y(2^k) = 0$. If this is the case we have a reason to believe that $Y \in C$ and if this is not the case we are sure that $Y \notin C$. We might of course be wrong but the measure of the set of all the infinite binary strings that can be elements of C according to our test is 2^{-n} . As a result we can be more and more confident that an infinite binary sequence is indeed in C if we increase n . If we define $U_n = \{X \in 2^\omega : \forall k < n X(2^k) = 0\}$ then $\{U_n\}_n$ indeed defines a Martin-Löf test and only the elements of C , which are clearly not random, fail this test.

You can think of a set U_n which is part of a Martin-Löf test as all the infinite binary strings that fail some computably enumerable statistical test with confidence 2^{-n} . We

want to be sure that only the infinite binary strings that actually fail the statistical test are elements of the Martin-Löf test. Therefore we want to have n go to infinity. This is done in a mathematically clean way by taking the intersection of all the $\{U_n\}_{n \in \mathbb{N}}$. This improves on the statistical approach of the previous section because we are not considering only one statistical property (normality) but in fact all effective statistical properties.

3.3 Paradigm 3: the unpredictability paradigm

The final way to define randomness we will consider, and perhaps the most intuitive, is that a random infinite binary string should be *unpredictable*. In common language, randomness is sometimes even used as a synonym for unpredictability. An event is called random if there is no way to predict its outcome. Similarly, an infinite binary string $X = x_0, x_1, x_2, x_3, \dots$ should be random if there is no way to predict one of its bits given any other bits. Another way to think about this is that one should not be able to win unlimited amounts of money when betting on the digits of a random infinite string. Below this intuition is formalised using martingales.

The unpredictability paradigm defines randomness by stating that an infinite binary string $X \in 2^\omega$ is not random if a martingale from some specific class of martingales succeeds on X . Of course, when considering all martingales, there will be a martingale succeeding on every infinite binary string and there will be no random sets left which is why we have to restrict the class of all martingales. Schnorr [26] therefore proposed considering only c.e. martingales. It was proven by Schnorr [26] that an infinite binary string $X \in 2^\omega$ is 1-random if and only if there is no c.e. martingale succeeding on it. A c.e. martingale is a martingale which is c.e. in the sense of paragraph 2.3.1.

Example 5. As an example of how we can use martingales to classify an infinite binary string as not 1-random, let us consider an infinite binary string X that has twice as many 1's as 0s. With this we mean that $\lim_{n \rightarrow \infty} \frac{\sum_{i < n} X(i)}{n} = \frac{2}{3}$. Such a string does not satisfy the law of large number and therefore we expect it to not be random. To illustrate why this string is not random using the unpredictability paradigm, let us define a betting strategy where we, at every stage of the game, bet 70% of our capital on the next digit being a 1 and the rest on the next digit being a 0. For every finite binary string σ the value of the martingale corresponding to our betting strategy is given by $d(\sigma) = 0.3^{\sigma_0} 0.7^{\sigma_1} 2^{|\sigma|}$ where σ_0 and σ_1 denote the number of zeroes and ones in σ respectively. Since X contains twice as many ones as zeroes we then have that for large enough n ,

$$d(X \upharpoonright n) = (0.7 \cdot 0.7 \cdot 0.3)^{\frac{n}{3}} 2^n = 1.176^{\frac{n}{3}} 2^n.$$

Therefore $\lim_{n \rightarrow \infty} d(X \upharpoonright n) = \infty$ which means that the martingale succeeds on X and that X is therefore not random.

3.4 Other notions of randomness

While the notion of 1-randomness is appealing because the three main paradigms agree on it, there are many other possible definitions of randomness. Here we will review some of those.

As the name implies, 1-randomness can be extended to n -randomness for any $n \in \mathbb{Z}_{>0}$ which uses generalisations of c.e. sets in its definition. However, if an infinite binary is not n -random then it is also not 1-random. Therefore it is only worth looking at the n -randomness of quantum mechanics after its 1-randomness has been established. Also, one could argue that 1-randomness is "random enough" and that it is not worth looking at stronger degrees of randomness. For these reasons, we will not go into n -randomness here but a full explanation can be found in chapter 6.8 of Algorithmic Randomness and Complexity [7].

Proving the randomness of quantum mechanics for a weaker randomness notion than 1-randomness would still be very interesting and worthwhile. Therefore, we will examine some of these weaker notions. The first weaker randomness definition we will consider, known as **Schnorr randomness**, uses the measure-theoretic paradigm in its definition. Schnorr randomness defines a modification of the Martin-Löf test, a Schnorr test, by requiring that $\mu(U_n) = 2^{-n}$ instead of $\mu(U_n) \leq 2^{-n}$. We then get the following definition:

Definition 5. (Schnorr [28]) A collection $\mathcal{A} \subseteq 2^\omega$ is called *Schnorr null* if there exists a uniformly c.e. sequence $\{U_n\}$ with $\mu(U_n) = 2^{-n}$ such that $\mathcal{A} \subseteq \bigcap_n U_n$. An infinite binary sequence X is Schnorr random if $\{X\}$ is not Schnorr null.

Schnorr randomness can also be defined using the unpredictability paradigm as was done by Schnorr [28]. This uses the concept of an **order**. This is a non-decreasing, unbounded function $h : \mathbb{N} \rightarrow \mathbb{N}$. We say a martingale d h -succeeds on an infinite binary string X if

$$\limsup_{n \rightarrow \infty} \frac{d(X \upharpoonright n)}{h(n)} = \infty.$$

An infinite binary string X is Schnorr random if there exist a computable martingale d and a computable order h such that d h -succeeds on X .

More generally, one convenient way to define other notions of randomness is by using the unpredictability paradigm and varying the complexity of the martingales that are considered. If there is no computable martingale that succeeds on an infinite binary string X then we call X **computably random**. We call X $O(T(n))$ -**random** if there is no martingale computable in $O(T(n))$ -time that succeeds on X . By varying the complexity of the martingales we obtain a spectrum of randomness degrees. It is interesting to investigate where quantum generated randomness fits in this spectrum.

4 Algorithmic randomness of the results of quantum mechanics

Suppose we consider an electron with its spin in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and suppose we measure $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$. Most physicists would tell us that we would randomly measure the spin to either be in the $|0\rangle$ or in the $|1\rangle$ direction. But if we repeat this procedure and generate a binary string by writing down in which direction we measure the particle, where will the randomness of this string then fit in the spectrum of randomness definitions from algorithmic randomness? Of course, algorithmic randomness

is concerned with infinite binary strings. Let us therefore consider a situation where we keep measuring these kinds of electrons and assign a 0 to a measurement of -1 (particle in the $|1\rangle$ state) and a 1 to a measurement of $+1$ (particle in the $|0\rangle$ state) to obtain an infinite binary string. If one does not want to work with this infinite binary string because only a finite number of measurements is possible, one can still wonder if the Kolmogorov complexity of a string of length N generated in this way is large or not.

According to the Born rule, the probability of measuring a 0 in the setting described above equals $\frac{1}{2}$. If one accepts these probabilities and assumes that they are the same and independent for each measurement, then one obtains that the infinite binary string is 1-random with probability 1. This is because, as a consequence of the existence of a universal Martingale-Löf test, the set of infinite binary strings that are not 1-random has measure 0. If one considers the Kolmogorov complexity of an N bit string then the probability that this is Kolmogorov random approaches 1 as N approaches infinity because almost all strings have high Kolmogorov complexity [3].

However, one can also interpret the Born rule as giving the relative frequency of the possible measurement outcomes and not the probabilities, as this relative frequency is all that is experimentally measurable. Then the Born rule only describes the fraction of the measurements that give a certain outcome if one repeats the same measurement a large number of times. This interpretation of the Born rule allows the outcomes to be described by a pseudo-random number generator provided it gives the correct statistics. If one allows this as possible or if one wants to avoid the use of the Born rule altogether, one might wonder if there are other methods to prove the randomness of the string described above. Below we will look at some literature in that direction. We will see that a large part of the literature tries to derive randomness purely from entanglement and the property of no signalling. This property states that it should not be possible to devise a method to communicate faster than light.

As we have seen in the previous section, there are many different degrees of randomness. For different purposes, different definitions of randomness can be applicable. While 1-randomness has the nice property of being defined using the three paradigms, the does not mean it is the right randomness notion for quantum mechanics. For this reason we will also look at results from the literature attempting to show that quantum mechanics is random for weaker randomness definitions.

4.1 No go theorems in quantum mechanics

The question if there can be hidden variables reproducing the outcomes of quantum mechanics has been around for a long time. In order to answer this question several so called no-go theorems where proven. These no go theorems exclude some class of functions from reproducing the results of quantum mechanics. Here we will briefly review the most important of these no go theorems. A far more exhaustive explanation of these theorems can be found in Landsman [13, ch 6].

4.1.1 The Kochen Specker theorem

The first no go theorem we will look at is the Kochen Specker theorem [12]. The KS theorem looks at a situation where we presume the existence of additional hidden states $x \in X$. These states determine the outcome of the measurement of an observable. This is described by functions $V_x : H_n(\mathbb{C}) \rightarrow \mathbb{R}$. Here $H_n(\mathbb{C})$ denotes the set of all self adjoint complex $n \times n$ matrices (operators on a finite dimensional Hilbert space). We have already made our first limitation on the class of hidden variable functions we are considering by having them only depend on the observable itself and not on other observables being co measured. This class of functions is called *non-contextual*.

The Kochen Specker theorem is concerned with *non-contextual quasi-linear hidden variables*. These non-contextual quasi-linear hidden variables are functions $V : H_n(\mathbb{C}) \rightarrow \mathbb{R}$ with the following properties:

1. $V(a)^2 = V(a^2)$ that is, V is dispersion-free
2. $V(I) \neq 0$, where I is the unit. V is normalised
3. For all $a, b \in H_n(\mathcal{C})$ that commute (i.e. $ab = ba$) and for all $s, t \in \mathcal{R}$ we have $V(sa + tb) = sV(a) + tV(b)$. This property is called quasi-linearity.

The KS theorem states that if the Hilbert space dimension is larger than 2, no non-contextual quasi-linear hidden variables exist. The proof of this can for example be found in [13].

The Kochen Specker theorem is often formulated in another equivalent way. For this we look at $\mathcal{P}_1(\mathcal{H})$, the set of all one-dimensional projectors on \mathcal{H} . Recall that one dimensional projectors are of the form $|\psi\rangle\langle\psi|$ for some $\psi \in \mathcal{H}$. This equivalent formulation looks at functions $V : \mathcal{P}(\mathcal{H}) \rightarrow \{0, 1\}$ with the property that if $M \subseteq \mathcal{P}_1(\mathcal{H})$ is a measurement, that is $\sum_{P \in M} P = I$ and the vectors $|\psi\rangle$ generating these projectors are perpendicular to each other, we have that $\sum_{P \in M} V(P) = 1$. You can think about this setting in the following way: a projector operator $|\psi\rangle\langle\psi|$ as asking the system if it is in state $|\psi\rangle$. The map V will predict if the particle will answer yes to this question, in this case V gives 1, or no in which case V gives 0. For each measurement the values $V(P)$ must sum to 1 because the particle can be in only one state at the same time and therefore only parallel to one of the $|\psi\rangle$ since those are perpendicular to each other. In this formulation, measurement non-contextuality implies as that $V(P)$ must be the same regardless of the other projector operators in the measurement with P . The Kochen Specker theorem now states that if the Hilbert space dimensions is greater than 2, maps $V : \mathcal{P}_1(\mathcal{H}) \rightarrow \{0, 1\}$ that are measurement non-contextual do not exist. This can be interpreted as the impossibility to predict along which basis vector of some orthonormal basis the system will be found after measurement.

4.1.2 The free will theorem

The free will theorem is a no-go theorem which replaces the non-contextuality assumption of the Kochen Specker theorem by certain locality assumptions. The theorem considers a situation with physicists, Alice and Bob, who are both measuring one half of an entangled state $\psi = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle + |2_A 2_B\rangle)$. We consider two entangled three

dimensional qutrits instead of the simpler qubits because the Kochen Specker theorem needs a Hilbert space dimension of at least 3 to hold. Alice and Bob both choose a basis to measure in, which we denote by x and y respectively. The free will theorem now modifies the assumptions of the Kochen Specker theorem to the following four:

1. **Determinism** states that there is a state space S and functions which describes the setting and the outcome of the experiment according to the following functions:

$$A : S \rightarrow X_A;$$

$$B : S \rightarrow X_B;$$

$$Z : S \rightarrow X_Z;$$

$$F : S \rightarrow X_G;$$

$$G : S \rightarrow X_F.$$

Here X_A and X_B are the sets of Alice's and Bob's measurement inputs, which in this case are the bases they can measure in. X_F and X_G are the output spaces. The function Z describes possible hidden variables. The first three functions then describe the outcome of the experiment according to the following functions:

$$\hat{F} : X_A \times X_B \times X_Z \rightarrow X_F;$$

$$\hat{G} : X_A \times X_B \times X_Z \rightarrow X_G,$$

which give the values of F and G according to $F(s) = \hat{F}(A(s), B(s), Z(s))$ and $G(s) = \hat{G}(A(s), B(s), Z(s))$.

2. **Freedom** means that the functions A , B and Z are independent. This means that for every triple $(x, y, z) \in X_A \times X_B \times X_Z$ there is some $s \in S$ such that $A(s) = x$, $B(s) = y$ and $Z(s) = z$. This requirement allows Alice and Bob to freely choose their measurement inputs and tells us that the hidden variable being used to describe the outputs of a certain measurement run does not depend on the measurement settings being used in that run.
3. **Nature** models the quantum mechanical predictions for the experiment. The system will be measured in only one of the basis vectors therefore $X_F = X_G = \{1, 2, 3\}$. The values of F and G denote in along which vector of the basis that is being measured in the system is found i.e. the first, second or third basis vector. Furthermore, if Alice or Bob changes only the sign of some of the basis vector this does not affect the outcome. This is because a projection operator does not change with a change of sign of the vector. Lastly, nature states that if Alice and Bob measure in the same basis, they will get the same result. This is because of the entangled state the system is in.
4. **Locality** is the assumption that replaces non-contextuality. It states that the outcome of Alice's experiment should be independent of Bob's measurement setting and vice versa. This can be described mathematically with a slight abuse of notation as $F(s) = \hat{F}(A(s), Z(s))$ and $G(s) = \hat{G}(B(s), Z(s))$.

The Free will theorem now states that **determinism**, **freedom**, **nature**, and **locality** are contradictory. This means that at least one of them must be false. For the proof I again refer to Landsman [13].

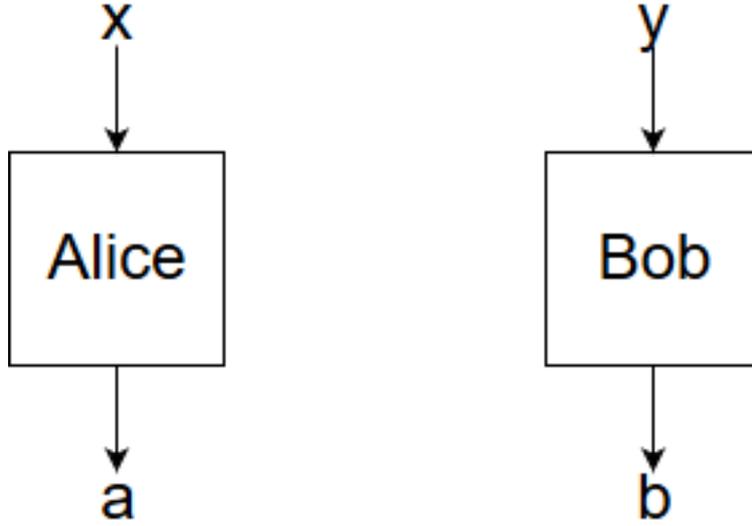


Figure 1: A schematic drawing of the situation being considered in Bell inequalities.

4.1.3 Bell inequalities

Finally, we discuss Bell inequalities, which also exclude the existence of hidden variables in quantum mechanics. But Bell inequalities do more, they provide a criterion on hidden variables independent from quantum theory. A far more thorough explanation of Bell inequalities than will be given below can be found in [24].

The setting of Bell inequalities is a situation with two agents, Alice and Bob, who are at different locations. Both have on them a measurement device which is treated as a black box. Alice's box takes an input $x \in X$ and gives an output $a \in A$ and Bob's box takes an input $y \in Y$ and then outputs $b \in B$. The situation is displayed in figure 1. We can look at the probabilities $P(a, b|x, y)$, the probability that the outputs of the two boxes are a and b given that the inputs were x and y . Without making any assumptions we can write

$$P(a, b|x, y) = \int \rho(\lambda|x, y)P(a, b|x, y, \lambda)d\lambda.$$

Here λ mathematically describes the process we use to describe the outcomes of the box and ρ is some positive function which integrates to 1. We assume that for each run of the experiment λ cannot use information about the inputs (x, y) used in that round. This is called **measurement independence** and is mathematically described by $\rho(\lambda|x, y) = \rho(\lambda)$. We call the boxes local if $P(a, b|x, y, \lambda) = P(a|x, \lambda)P(b|y, \lambda)$. This means that the output of box A can only depend on the input of box A and on λ but, importantly, cannot depend on the input and output of box B . We say the boxes are **deterministic** if the probabilities $P(a, b|x, y, \lambda)$ are either zero or one. If we want to prevent the boxes from being able to signal we need that $P(a|x, y, \lambda) = P(a|x, \lambda)$ for all a and that $P(b|x, y, \lambda) = P(b|y, \lambda)$ for all b .

Let us now look at the simplest non trivial case, where $X = Y = A = B = \{0, 1\}$. Under the constraints of measurement independence, locality and non-signalling described

above, one can derive the so called CHSH inequality, named after Clauser, Horne, Shimony and Holt [5]. This inequality is given by

$$I = E_{00} + E_{01} + E_{10} - E_{11} \leq 2$$

where $E_{xy} = P(a = b|x, y) - P(a \neq b|x, y)$. E_{xy} is often called the **correlation coefficient**. Under the assumption of measurement independence, all local non-signalling boxes will satisfy this inequality. In particular all deterministic boxes satisfy this inequality, since all non-local deterministic boxes can signal. However, the mathematical formalism of quantum theory predicts an upper bound of $2\sqrt{2}$ [4], which is bigger than 2. Therefore, quantum measurements can in principle violate the CHSH inequality. In fact, Gisin [9] proved that if Alice and Bob are performing measurements on an entangled quantum systems of the form $|\psi\rangle = \sum_{k=0}^{d-1} c_k |k\rangle$ they will then necessarily violate the CHSH inequality.

Example 6. As an example of how quantum theory predicts measurements that violate the CHSH inequality, let us consider the following state of two entangled qubits

$$|\psi\rangle = |0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle.$$

Suppose that Alice measures in an orthonormal basis including \vec{x} and Bob in an orthonormal basis including \vec{y} . We then have

$$\begin{aligned} E_{\vec{x}\vec{y}} &= P\left((a, b) = (1, 1)|\vec{x}, \vec{y}\right) + P\left((a, b) = (0, 0)|\vec{x}, \vec{y}\right) \\ &\quad - P\left((a, b) = (1, 0)|\vec{x}, \vec{y}\right) - P\left((a, b) = (0, 1)|\vec{x}, \vec{y}\right) \end{aligned}$$

We can write this as

$$\begin{aligned} E_{\vec{x}\vec{y}} &= P(a = 1|\vec{x}, \vec{y}) \left(P(b = 1|\vec{x}, \vec{y}, a = 1) - P(b = 0|\vec{x}, \vec{y}, a = 1) \right) \\ &\quad + P(a = 0|\vec{x}, \vec{y}) \left(P(b = 0|\vec{x}, \vec{y}, a = 0) - P(b = 1|\vec{x}, \vec{y}, a = 0) \right) \end{aligned}$$

We have that

$$P(b = 1|\vec{x}, \vec{y}, a = 1) - P(b = 0|\vec{x}, \vec{y}, a = 1) = -\vec{x}\vec{y}$$

and a similar expression for $a = 0$. Together with

$$P(a = 1|\vec{x}, \vec{y}) + P(a = 0|\vec{x}, \vec{y}) = 1$$

we end up at $E_{\vec{x}\vec{y}} = -\vec{x}\vec{y}$

Now choosing $\vec{x}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\vec{x}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\vec{y}_1 = \begin{pmatrix} -\sqrt{1/2} \\ -\sqrt{1/2} \end{pmatrix}$, and $\vec{y}_2 = \begin{pmatrix} -\sqrt{1/2} \\ \sqrt{1/2} \end{pmatrix}$ gives us $I = 2\sqrt{2}$ which violates the CHSH inequality.

4.2 Previous results about the algorithmic randomness of quantum mechanics

In this section we will look at previous results concerning the algorithmic randomness of quantum measurement outcomes. Unfortunately, there is no definite proof of the algorithmic randomness of quantum measurement outcomes yet. However, there are results in the right direction. We will look at these and investigate what they do tell us.

4.2.1 Senno's thesis

Perhaps one of the most promising results so far is Senno's thesis [29], in which he proves that faster than light communication is possible if we assume quantum mechanics to be computable and non-local. While interesting, this result is very weak result.

Senno starts out from a Bell like scenario with two observers, Alice and Bob, who were once together but then flew away in their spaceships in opposite directions. He supposes that both have access to a box. Alice's box takes inputs in X and then gives an output in A whereas Bob's box has inputs in Y and outputs in B . Senno only considers the simplest non trivial case, namely $A = B = X = Y = \{0, 1\}$. He then assumes that there are computable functions $\mathcal{A} : X \times Y \times \mathbb{N} \rightarrow A$ and $\mathcal{B} : X \times Y \times \mathbb{N} \rightarrow B$ that give the output of the n -th round of Alice's and Bob's box respectively. He also assumes that the boxes are non-local, which means that there are infinitely many n for which there is a y such that $\mathcal{B}(0, y, n) \neq \mathcal{B}(1, y, n)$ and that there are infinitely many n for which there is an x such that $\mathcal{A}(x, 0, n) \neq \mathcal{A}(x, 1, n)$. This non-locality is required because no local theory can reproduce the results of quantum mechanics as we have seen in the previous section. Of course, if Alice and Bob knew how to compute A and B they could signal. However, they do not know how to do that yet.

Senno gives a protocol with which Alice and Bob can learn how to compute these functions. The protocol works by $O(T(n))$ -randomly switching between learning rounds and signalling rounds. Here $T(n)$ is such that \mathcal{A} and \mathcal{B} are computable in $O(T(n))$ time. In the learning rounds, Alice and Bob give inputs they agreed upon before they left each other to improve their guesses of \mathcal{A} and \mathcal{B} . In the signalling rounds they try to signal part of their message using their guesses of \mathcal{A} and \mathcal{B} . The protocol is too complicated to explain here fully, but it results in Alice and Bob being able to reliably signal.

The first issue that appears, as also noted by Senno himself, is that the proof assumes a time computational complexity bound on the computable function that is supposed to compute all the box outputs. The method described by Senno to achieve faster than light communication no longer works if the time computational complexity is higher than some fixed bound that two persons attempting to signal to each other agreed on. It must be noted that there is no limit on this bound which the persons attempting to signal agree on. However, as long as the time computational complexity of the function describing quantum mechanics is unknown, they will not be able to tell in advance if their bound is good enough.

A second issue is that non-computable functions do not necessarily output 1-random (or computationally random) sequences. We will illustrate this using an example I found in Calude and Svozil [2]:

Example 7. Let T_1, T_2, T_3, \dots be an enumeration of all Turing machines. Let us now define an infinite binary sequence $H = h_1 h_2 h_3 \dots$ where $h_i = 1$ if Turing machine T_i halts on input i and $h_i = 0$ if it does not. Since the halting problem is uncomputable, so will be H . However, we can define a martingale that succeeds on H . To do this, consider an infinite sequence U_1, U_2, U_3, \dots of Turing machines known to halt (for example the Turing machines implementing addition by a fixed constant). Now define a martingale d by letting d be constant unless $T_i = U_j$ for some j , in which case we set $d(h_1 \dots h_{i-1} 1) = 2d(h_1 \dots h_{i-1})$ and $d(h_1 \dots h_{i-1} 0) = 0$. In other words, we split our bets

to make sure we neither win nor lose money, unless we are sure that the next Turing machine will halt, in which case we bet all our money that it will halt. Since there are infinitely many Turing machines of which we are sure they will halt, we can make an arbitrary amount of money using this strategy, so H cannot be 1-random. Effectively, since H is essentially the halting problem which is c.e. and therefore contains an infinite computable subset, it is not 1-random.

Another example of a string that is not computable but also not 1-random is a diluted random string. If we take a 1-random string and insert a zero at every even location it will no longer be 1-random. However, it will also not be computable as the odd digits form a 1-random string.

However, one could consider the property of not being the output of a computable function a very weak notion of randomness. Senno's proof is not a proof of 1-randomness, but it is definitely a step in the right direction.

4.2.2 Yurtsever's article

Another interesting paper regarding our question is a paper by Yurtsever [32]. In his article Yurtsever claims to prove that a bit string generated by measurements on a certain quantum mechanical system is Kolmogorov random with a probability approaching 1 as the length of the string approaches infinity. However, the proof that is given in the article is lacking in several points. I will first give a brief overview of Yurtsever's sketch of proof, and then point out where it is lacking.

Yurtsever considers entangled spin- $\frac{1}{2}$ particles with a quantum state $|\psi\rangle$ given by

$$|\psi\rangle = \alpha|\uparrow_1\rangle|\downarrow_2\rangle + \beta|\downarrow_1\rangle|\uparrow_2\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$.

Yurtsever considers the general case, and uses the notion of p -compressability to do so. This notion is too involved to go into here but it reduces to the plain Kolmogorov complexity in the case where $\alpha = -\beta = \frac{1}{\sqrt{2}}$. For this reason I will only discuss the case where this holds.

Yurtsever considers a stream of such particles being produced by a (stationary) source. Of each pair in the stream, the two particles fly off in opposite directions and are then measured with respect to the up-down basis by Alice or Bob. Alice and Bob are both generating a binary string from their measurements. They have agreed that when Alice measures spin up she adds a 1 to her string, and otherwise a 0. Bob does the opposite: when he measures spin up he adds a 0 to his string, and otherwise a 1. Because of the entanglement, when Bob measures spin up he is sure that Alice will measure spin down, and vice versa. A consequence of this is that Alice and Bob will both generate the same binary string. What Yurtsever tries to do is use the entanglement together with the assumption that quantum mechanics is not random to create a faster than light communication channel between Alice and Bob.

To construct this communication channel, Yurtsever considers the probability p_N that an N -bit segment of Bob's or Alice's string is Kolmogorov random. In order to transfer bits of information from Bob to Alice, Alice and Bob agree to interpret an N -bit segment as a 1 if it is Kolmogorov random and as a 0 if it is not. In order to send Alice a 1,

Yurtsever says that Bob should do nothing and keep measuring his stream of particles with respect to the up-down basis. This will result in a 1 being sent with a probability p_N . To send a 0, Bob should "scramble" his string: He should use some method (Yurtsever suggests a roulette wheel) to generate a random "template" sequence of length T larger than N . This template should almost surely be Kolmogorov random. Bob should then prepare a sequence of N measurement directions using this template sequence as a random number generator. He then performs his next N measurements along the bases associated with the directions from the random sequence. Yurtsever now claims that the string measured by Bob using the "scrambling" process is almost surely Kolmogorov random and that Alice's string, which is now different from Bob's, will also be almost surely Kolmogorov random.

This last claim is the point of the argument which is most in need of clarification. It is not obvious, and possibly not even true, that Bob's string will (almost surely) be Kolmogorov random after the scrambling, especially since it was just assumed that quantum measurements will in general not give a Kolmogorov random string. It is also unclear how this scrambling would affect Alice's string, as it will then be different from Bob's. This becomes even stranger when you consider that quantum mechanics is non-signalling and that thus when Bob changes his measuring basis it will not affect the statistics of Alice's experiment. This is also noted by Yurtsever but he does not explain how this is circumvented by considering the complexity of the measured strings. In the article, Yurtsever refers to a manuscript in preparation which was supposed to provide a more detailed rigorous analysis. Unfortunately, this manuscript has never appeared.

After this insufficiently supported part of his sketch of proof, Yurtsever continues by stating that Alice could use an approximation of Chaitin's Ω to determine if her N -bit string segment is Kolmogorov random or not. Because Alice uses an approximation of Ω there is a chance that she incorrectly characterises a non Kolmogorov random string segment as Kolmogorov random, but according to Yurtsever this does not disrupt the possibility of communication. If Bob scrambling his measurements does change the probability that Alice receives a Kolmogorov random N -bit string segment, then this makes up a (noisy) communication channel. Yurtsever then proceeds by stating that the principles of special relativity forbid such a channel and that therefore any N -bit string segment must almost surely be Kolmogorov random.

To conclude, Yurtsever approaches the problem from a different angle by considering the probability that a finite bit segment is Kolmogorov random. Unfortunately, he uses claims that are insufficiently supported by proofs to derive his result. The manuscript in preparation he uses as a reference to support his claims has not appeared. Consequently, his paper does not answer our question, although it could serve as a starting point for future attempts at proving quantum mechanics to be random.

4.2.3 Calude & Svozil

Another article which claims to prove that the results of quantum measurements are random is an article by Calude and Svozil [2]. In the article, the authors consider a quantum experiment which at each stage generates a 1 or a 0 with equal probability. This is repeated to obtain an infinite binary sequence $X = x_1 x_2 x_3 \dots$. The randomness of this

string is studied.

First, they apply the second formulation of the Kochen Specker theorem above. They reason that, if the Hilbert space dimension is greater than three, there is no non-contextual way to predict in which one dimensional subspace a system will be found. Therefore, if a bit string is generated by measurement of a quantum system the bit string cannot be the output of a non-contextual function since if it were it would violate the KS theorem. They then conclude that an infinite binary string generated by quantum measurements cannot be the output of a non-contextual computable function.

One issue with their proof is that it only considers non-contextual deterministic computations. It would still be possible for quantum mechanics to be the output of a contextual computation. The authors do not go into detail about this possibility. One way around this would be to use the free will theorem which drops the non-contextuality assumption. However, it introduces other assumptions which can be dropped. For example, the free will theorem does not exclude a non-local deterministic theory from replicating the results of quantum mechanics.

Furthermore, the argument from Calude and Svozil suffers from the same problem as Senno's argument: non-computability does not imply randomness. Calude and Svozil admit this and give the example that was also used above to show this fact.

4.2.4 Rogers

The last theoretical contribution on the randomness of quantum measurements we will consider is a paper by C. Rogers [23]. This paper is different from the papers we looked at above in that it does not try to prove the randomness of quantum measurement outcomes. Instead, Rogers argues that it is impossible to prove the randomness of quantum mechanics. She states that it is not possible to prove the Kolmogorov randomness of infinitely many finite binary strings. We have already seen this fact in Barzdin's theorem [1]. Rogers gives a proof very similar to Barzdin's, but does not cite him. She then argues that because of this it is impossible to prove the randomness of quantum measurements. She notes that this does not mean that measurements in quantum theory are not random but she does suggest that this might favour interpretations of quantum mechanics that do not claim measurement outcomes are random over interpretations that do such as the "textbook" interpretation.

While it is true that it is impossible to prove the randomness of infinitely many finite binary strings, that does not mean we should give up. Results about the probability to obtain a Kolmogorov random string, like Yurtsever tried to give, are not impossible. Neither are results about the probability to obtain a 1-random string. We already saw that this probability is 1 in the case where we interpret the Born rule as giving probabilities. However, results like these still have to be proven if we interpret the Born rule as only describing the statistics of the measurement outcomes.

To conclude, Rogers is right in her claim that we cannot prove the randomness of infinitely many finite bit strings generated by some quantum measurement. However, this does not mean it is also impossible to derive meaningful results about the randomness of strings generated by quantum measurements. Therefore, interpretations of quantum mechanics that do not make any statements about randomness should not be favoured

over interpretations that do.

5 Randomness of quantum random number generators

5.1 ID quantique's *quantis*

In the previous section we saw that the literature does not prove quantum mechanics to be random from its entanglement and non-signalling properties. However, in practice the supposed randomness of quantum mechanics is still used. In this section we will investigate its use in quantum random number generators. We will also consider justifications for the randomness of these generators.

Random numbers are of vital importance for many applications, such as cryptography. While pseudo-random number generators work for many of such purposes, there are also many situations in which these do not suffice, as they can lead to security breaches. For this reason it is important to look at other methods of generating random numbers. One company with the name ID quantique (IDQ) is selling random number generators based on quantum mechanics. These provide random numbers used in many applications including the Swiss national lottery. But how do they know that the quantum random numbers their machines generate are actually random? That is the question we will investigate below.

ID quantique has published a white paper [22] in which they justify their claim that their quantum random number generator is superior to software based pseudo random number generators and generators based on classical physics. In this paper they start out claiming that an infinite binary sequence is random if there is no finite computer program producing the sequence. This definition makes no sense from an algorithmic randomness perspective. Suppose we have an infinite binary string whose even digits are always a 0 and whose odd digits are not computable. According to *quantis'* definition this is a random sequence but is it easy to see that there is a betting strategy succeeding on this string. They then discard this definition as useless because it is impossible to produce and process infinite sequences. They also discard the notion of Kolmogorov randomness (which they formulate in their own way) because it is formally impossible to check the randomness of a finite string (they are probably referring to the immunity of the set of Kolmogorov random finite strings here). To avoid these difficulties, ID quantique turns to "practical" definitions of randomness. They give two different definitions of this, one by Knuth[11] and one by Schneier[25]. Knuth's view is that a sequence of random numbers is a sequence of independent numbers with a specified distribution and a specified probability of falling into any given range of values. According to Schneier, a sequence of random number should have the same statistical properties as random bits, be unpredictable, and it should be impossible to reproduce such a sequence. IDQ emphasises that the numbers in a random sequence should not be correlated. Knowing any number of the digits should not help in predicting any other digit. IDQ states that when they mention random numbers they mean numbers satisfying these "practical" definitions of randomness.

IDQ proceeds by reviewing the randomness of software based random number generators or pseudo-random number generators. These are algorithms which, when fed with an initial value (called a seed), produce a sequence of numbers. The idea with pseudo-random number generators is that this resulting sequence appears to be random, which gives it the name pseudo-random. Of course, full knowledge of the seed and the algorithm is all we need to know the output string, so it is definitely not 1-random. Nevertheless, pseudo-random number generators are designed to imitate randomness as closely as possible. That is, they pass most statistical tests. However there will always be a test at which a pseudo-random number generator fails.

IDQ then turns to their quantum random number generator, the *quantis*. They claim that this machine does, in contrast to software-based (i.e. algorithmic) random number generators, output truly random numbers. They justify this claim in two ways.

First, they state that *quantis*' output must be random because it is based quantum on mechanics, which they claim is intrinsically random. As this claim is exactly what we are investigating, this does not help.

Second, they state that *quantis* passes all statistical tests but they give no justification to why this would be the case. Presumably, they only mean that *quantis* has passed all statistical tests it has been exposed to so far. Admittedly, it has passed all the tests it was exposed to by the Swiss Federal Bureau of Metrology (METAS) and other institutions. However it is not impossible that it will fail some other statistical test. Additionally, it is also possible to design a software based random number generator passing all the test *quantis* has passed. Therefore this is no proof of the randomness of *quantis*.

5.2 Random numbers certified by Bell's theorem

One article which proposes an experimental way to test the randomness of an quantum random number generator is 'Random number certified by Bell's theorem' by Pironio *et al.* [21]. In the article, the authors state that an experiment violating a Bell inequality guarantees that the outcomes were not predetermined.

The authors look at the simplest case, the case of the CHSH inequality which we have looked at above. Recall that this inequality holds for all local theories and that all deterministic theories that are non-local could in principle allow for signalling. The inequality is given by

$$I = E_{00} + E_{01} + E_{10} - E_{11} \leq 2$$

where $E_{xy} = P(a = b|x, y) - P(a \neq b|x, y)$. The authors suggest performing an experiment to find the values of these $E_{x,y}$. They suggest to generate the the measurement inputs (x, y) using by an independent and identically distributed (i.i.d.) probability distribution $P(x, y)$. One can then approximate $E_{x,y}$ as $(N(a = b|x, y) - N(a \neq b|x, y)) / P(x, y)$. Here $N(a = b|x, y)$ is the amount of times that the outputs a and b were equal and the inputs where x and y . $N(a \neq b|x, y)$ is defined analogously.

Let us look at a situation with two quantum random number generators which each generate their random numbers from an binary input and by measuring one part of an entangled system. We can calculate the approximations to $E_{x,y}$. If these violate a Bell inequality, then the two quantum random number generators cannot be generated by a local deterministic process. Violations of the Bell inequality have been observed (see for

example [10]). Therefore, one can conclude that no local deterministic theory can fully describe quantum mechanics.

The authors state that while the string itself might not pass one of the usual statistical tests, it still contains randomness that can be extracted by a randomness extractor to generate randomness. These extractors are pieces of software that make a string of bits appear more random. However, one issue is that randomness extractors are ultimately algorithms, fully deterministic and therefore cannot produce a 1-random string from a non 1-random string. For this reason the described method cannot be reliably used to generate a 1-random string.

Another issue one could have with this method is its circular nature. To generate random numbers we need an i.i.d. probability distribution to choose our inputs. This is also what the authors say. According to them their method is a randomness amplification method that can be used to generate more randomness from some initial randomness. However, one could argue that if randomness is fundamentally unavailable this method cannot be used to generate randomness.

6 Conclusion

We have seen that if we interpret the Born rule in a naive way and believe that it tells us the probabilities for each individual measurement, there will definitely be quantum measurements that, when repeated, generate random strings. However, if we do not have this naive approach to the Born rule, but instead see it as a description of the statistics of the measurement outcomes, or refuse to use it altogether, it is not so easy to show that these measurements exist. We also looked at proving the existence of these measurements only from the entanglement and the non-signalling properties of quantum theory. Finally, we looked at an experimental method to support the randomness of some quantum measurements.

Senno proved that if there were a deterministic and non-signalling quantum theory the deterministic function giving the predictions would have to be non-computable [29]. This means that every infinite binary sequence generated by repeatedly performing some quantum measurement cannot be the output of a computable function. While this does not imply randomness according to the definitions of randomness we looked at, it can be seen as a proof of a very weak form of randomness.

This result by Senno is supported by Calude and Svozil [2]. Additionally, experimental observations of violations of Bell inequalities [10] support the idea that the outcome of some quantum measurements definitely cannot be described by a deterministic process. However, we also saw that not being the result of a deterministic function is not enough to be random in the sense of any of the randomness definitions given by algorithmic randomness.

An attempt at proving a stronger result about the randomness of quantum measurements was made by Yurtsever. He tried to prove that a finite binary string generated by measurements on a qubit entangled with another qubit is Kolmogorov random with a probability approaching 1 as the length of the string approaches infinity. Unfortunately, he made two insufficiently supported claims which render his proof incomplete.

All in all, we can conclude that there are quantum measurements that cannot be the result of a deterministic process. We even have a method to experimentally check this for some setup. However, this is not enough to guarantee randomness in an algorithmic sense. More work is needed to show if there are quantum measurements that can be used to generate algorithmically random sequences.

References

- [1] Ya. M. Barzdin. “Complexity of programs to determine whether natural numbers not greater than n belong to a recursively enumerable set”. In: *Soviet Mathematics Doklady*. Vol. 9. 1251-1254. 1968, p. 122.
- [2] C. S. Calude and K. Svozil. “Quantum randomness and value indefiniteness”. In: *arXiv e-prints* (Nov. 2006).
- [3] G.J. Chaitin. “A theory of program size formally identical to information theory”. In: *Journal of the ACM* 22 (1975), pp. 329–340.
- [4] B. S. Cirel’son. “Quantum generalizations of Bell’s inequality”. In: *Letters in Mathematical Physics* 4.2 (1980), pp. 93–100.
- [5] J. F. Clauser et al. “Proposed experiment to test local hidden-variable theories”. In: *Physical review letters* 23.15 (1969), p. 880.
- [6] P. Diaconis, S. Holmes, and R. Montgomery. “Dynamical bias in the coin toss”. In: *SIAM review* 49.2 (2007), pp. 211–235.
- [7] R. G. Downey and D. R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer, 2010.
- [8] R. Downey et al. “Calibrating randomness”. In: *Bulletin of Symbolic Logic* 12.3 (2006), pp. 411–491.
- [9] N. Gisin. “Bell’s inequality holds for all non-product states”. In: *Physics Letters A* 154.5-6 (1991), pp. 201–202.
- [10] B. Hensen et al. “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres”. In: *Nature* 526.7575 (2015), p. 682.
- [11] D. E. Knuth. “The Art of Computer Programming, Vol. 2, Addison-Wesley”. In: *Reading, MA* (1973), p. 51.
- [12] S. Kochen and E. P. Specker. “The problem of hidden variables in quantum mechanics”. In: *The logico-algebraic approach to quantum mechanics*. Springer, 1975, pp. 293–328.
- [13] K. Landsman. *Foundations of quantum theory: from classical concepts to operator algebras*. Cham: Springer International Publishing, 2017.

- [14] L. A. Levin. “Laws of information conservation (nongrowth) and aspects of the foundation of probability theory”. In: *Problemy Peredachi Informatsii* 10.3 (1974), pp. 30–35.
- [15] L. A. Levin. “Some theorems on the algorithmic approach to probability theory and information theory”. In: *arXiv preprint arXiv:1009.5894* (2010).
- [16] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. Springer-Verlag, 1993.
- [17] G. Markowsky. “The sad history of random bits”. In: *Journal of Cyber Security and Mobility* 3.1 (2014), pp. 1–24.
- [18] R. v. Mises. “Grundlagen der Wahrscheinlichkeitsrechnung”. In: *Mathematische Zeitschrift* 5.1 (Mar. 1919), pp. 52–99.
- [19] J. von Neumann. “Various techniques used in connection with random digits”. In: *John von Neumann, Collected Works* 5 (1963), pp. 768–770.
- [20] P. Martin-Löf. “The definition of random sequences”. In: *Information and Control* 9.6 (1966), pp. 602–619.
- [21] S. Pironio et al. “Random numbers certified by Bell’s theorem”. In: *Nature* 464.7291 (2010), p. 1021.
- [22] *Random number generation using quantum physics*. Tech. rep. Geneva, Switzerland: ID Quantique, Apr. 2010, p. 8. URL: www.idquantique.com.
- [23] C. Rogers. “Quantum Measurements Cannot be Proved to be Random”. In: *ArXiv e-prints* (Aug. 2010). arXiv: 1008.5022 [quant-ph].
- [24] V Scarani. “The device-independent outlook on quantum physics”. In: *Acta Physica Slovaca* 62.4 (2012), pp. 347–409.
- [25] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 2007.
- [26] C. P. Schnorr. “A unified approach to the definition of random sequences”. In: *Mathematical systems theory* 5.3 (Sept. 1971), pp. 246–258.
- [27] C. P. Schnorr. “Process complexity and effective random tests”. In: *Journal of Computer and System Sciences* 7.4 (1973), pp. 376–388.
- [28] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit: eine algorithmische Begründung der Wahrscheinlichkeitstheorie*. Vol. 218. Springer-Verlag, 1971.
- [29] G. I. Senno. “Una perspectiva teórico-computacional sobre fundamentos de la información cuántica”. URL: https://digital.bl.fcen.uba.ar/download/tesis/tesis_n6349_Senno.pdf.
- [30] A. M. Turing. “On Computable Numbers, with an Application to the Entscheidungsproblem”. In: *Proceedings of the London Mathematical Society* s2-42.1 (Jan. 1937), pp. 230–265.

- [31] J. Ville. *Étude Critique de la Notion de Collectif*. Gauthier-Villars, 1939.
- [32] U. Yurtsever. “Quantum mechanics and algorithmic randomness”. In: *Complexity* 6.1 (2000), pp. 27–34.