

How Real is Incomputability in Physics?

José Manuel Agüero¹ Trejo, Cristian S. Calude¹, Michael J. Dinneen¹,
Arkady Fedorov^{2,3}, Anatoly Kulikov^{2,3}, Rohit Navarathna^{2,3}, Karl Svozil⁴

¹School of Computer Science, University of Auckland, New Zealand

²School of Mathematics and Physics, University of Queensland, Australia

³ARC Centre of Excellence for Engineered Quantum Systems, Queensland, Australia

⁴Institut für Theoretische Physik, TU Wien, Vienna, Austria

Abstract

A physical system is determined by a finite set of initial conditions and “laws” represented by equations. The system is computable if we can solve the equations in all instances using a “finite body of mathematical knowledge”. In this case, if the laws of the system can be coded into a computer program, then given the initial conditions of the system, one can compute the system’s evolution.

Are there incomputable physical systems? This question has been theoretically studied in the last 30–40 years.

In this paper, we experimentally show for the first time the strong incomputability of a quantum experiment, namely the outputs of a quantum random number generator. Moreover, the experimental results are robust and statistically significant.

Keywords: Incomputability, Localised Kochen-Specker Theorem, 3D-QRNG physical implementation, testing incomputability

1. Introduction

Incomputability in physics has been studied by many authors [55, 56, 58, 39, 23, 45, 19, 21, 64, 38, 22, 10, 42, 30, 36, 62, 42, 15, 37, 1, 3, 27, 8, 31]. The results in all these articles are theoretical, so following Einstein [25],

Physics constitutes a logical system of thought which is in a state of evolution ... The justification (truth content) of the system rests in the proof of the usefulness of the resulting theorems on the basis of sense experiences, where the relations of the latter to the former can only be comprehended intuitively.

we can ask: *what is their justification?* The word “real” in the title of this article means “a justification of incomputability based on usefulness”.

Justifying “usefulness” is not easy. Indeed, for sufficiently complex systems (even reversible) determinism on a “one-by (to)-one” evolution basis does not imply predictability [54]. For example, take the n -body problem: the series of solutions [61, 44, 53, 59, 60] could be “very slowly” convergent [24], or even encode the Halting Problem [57].

In this article, we study experimentally the outputs of a quantum random number generator (QRNG), which was theoretically proven to be strongly incomputable, the only QRNG among many candidates – see [34, 35, 11, 55, 29, 28]. Our main results are: a) we experimentally show the strong incomputability of a quantum experiment, namely the outputs of a quantum random number generator, a significant improvement of the results in [2] and b) we prove that the experimental results are robust and statistically significant.

We use a located form of the Kochen-Specker Theorem [1, 5, 6] to derive a class of quantum protocols producing quantum random bits [8, 9]. Theoretically, it was proved that every infinite sequence generated with these quantum protocols is strongly incomputable – no algorithm computing any bit of such a sequence can be proved correct, hence the sequence is maximally unpredictable [5]. This result is more robust than the ones in the literature and satisfies Einstein’s requirement of justification: the experimental results presented here confirm and complement the theoretical results of incomputability and unpredictability and, quite significantly, the choice of physical assumptions.

The paper is organised as follows. In Section 2, we present the theoretical framework for the Localised Kochen-Specker Theorem, allowing the construction of strongly incomputable sequences via measurements of value-indefinite observables. In Section 3, we use a standard superconducting transmon system to implement logical states as qutrits and realise the theoretical quantum protocols in Section 2. In Section 5, we present a method to empirically show the incomputability of the outputs generated in Section 3. The last Section 6, we briefly discuss the results presented in this article and suggest further continuations.

2. 3D-QRNG – Theory

In this section, we present the theoretical framework allowing the construction of value-indefinite observables, their tolerance to measurement errors and the certification of the degree of randomness of their outcomes.

2.1. Notation and definitions

The set of positive integers will be denoted by \mathbb{N} . Consider the alphabet $A_b = \{0, 1, \dots, b-1\}$, where $b \geq 2$ is an integer; the elements of A_b are the digits used in natural positional representations of numbers in the interval $[0, 1)$ at base b . By A_b^* and A_b^ω we

denote the sets of (finite) strings and (infinite) sequences over the alphabet A_b . Strings will be denoted by x, y, u, w ; the length of the string $x = x_1x_2 \dots x_m$, $x_i \in A_b$, is denoted by $|x|_b = m$ (the subscript b will be omitted if it is clear from the context); A_b^m is the set of all strings of length m . Sequences will be denoted by $\mathbf{x} = x_1x_2 \dots$; the prefix of length m of \mathbf{x} is the string $\mathbf{x}(m) = x_1x_2 \dots x_m$. Strings will be ordered quasi-lexicographically according to the natural order $0 < 1 < 2 < \dots < b-1$ on the alphabet A_b . For example, for $b = 2$, we have $0 < 1 < 00 < 01 < 10 < 11 < 000 \dots$. We assume knowledge of elementary computability theory over different size alphabets [13].

By \mathbb{C} , we denote the set of complex numbers. We then fix a positive integer $n \geq 2$ and let $O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space \mathbb{C}^n .

A set $C \subset O$ is a *context* of O if C has n elements and for all $P_\psi, P_\phi \in C$ with $P_\psi \neq P_\phi$, $\langle \psi | \phi \rangle = 0$. A *value assignment function* (on O) is a partial function $v : O \rightarrow \{0, 1\}$ assigning values to some (possibly all) observables in O . The partiality of the function v means that $v(P)$ can be 0, 1 or indefinite. An observable $P \in O$ is *value definite* (under the assignment function v) if $v(P)$ is defined, i.e. it is 0 or 1; otherwise, it is *value indefinite* (under v). Similarly, we call O *value definite* (under v) if every observable $P \in O$ is value definite.

We then fix a positive integer $n \geq 2$ and let $O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space \mathbb{C}^n . A set $C \subset O$ is a *context* of O if C has n elements and for all $P_\psi, P_\phi \in C$ with $P_\psi \neq P_\phi$, $\langle \psi | \phi \rangle = 0$. A *value assignment function* (on O) is a partial function $v : O \rightarrow \{0, 1\}$ assigning values to some (possibly all) observables in O . The partiality of the function v means that $v(P)$ can be 0, 1 or indefinite. An observable $P \in O$ is *value definite* (under the assignment function v) if $v(P)$ is defined, i.e. it is 0 or 1; otherwise, it is *value indefinite* (under v). Similarly, O is *value definite* (under v) if every observable $P \in O$ is value definite.

2.2. The quantum protocol

The protocol is simple: *localise a value indefinite observable, measure it, and start again afresh.*

2.3. Localised Kochen-Specker Theorem

We assume the following premises to localise a value indefinite observable.

- **Admissibility.** This assumption guarantees agreement with quantum mechanics predictions. Fix a set O of one-dimensional projection observables on \mathbb{C}^n and the value assignment function $v : O \rightarrow \{0, 1\}$. Then v is *admissible* if for every context C of O , we have that $\sum_{P \in C} v(P) = 1$. Accordingly, only one projection observable in a context can be assigned the value 1.

- **Non-contextuality of definite values.** Every outcome obtained by measuring a value definite observable is *non-contextual*, i.e. it does not depend on other compatible observables, which may be measured alongside it.
- **Eigenstate principle.**¹ If a quantum system is prepared in the state $|\psi\rangle$, then the projection observable P_ψ is value definite.

Theorem 1 (Localised Kochen-Specker Theorem [4, 5, 37, 8]). *Assume a quantum system prepared in the state $|\psi\rangle$ in a dimension $n \geq 3$ Hilbert space \mathbb{C}^n , and let $|\phi\rangle$ be any quantum state such that $0 < |\langle\psi|\phi\rangle| < 1$. If the following three conditions are satisfied: i) admissibility, ii) non-contextuality and iii) eigenstate principle, then the projection observable P_ψ is value indefinite.*

Theorem 1 has two major consequences:

1. it shows how to construct a value indefinite observable effectively,
2. it guarantees that the status of “value-indefiniteness” is invariant under minor measurement errors: this is a significant property as no measurement is exact.

We note that Theorem 1, as the original Kochen-Specker Theorem [33], is not valid in \mathbb{C}^2 , hence the requirement to work in \mathbb{C}^3 .

How “good” is such a 3D-QRNG, i.e. what randomness properties can be *certified* for their outcomes? For example, can we prove that the outcomes of the 3D-QRNG are “better” than the outcomes produced by *any* pseudo-random number generator (PRNG)? For certification, we use the following assumption:

- **epr principle:** If a repetition of measurements of an observable generates a computable sequence, then these observables are value definite.

Based on the Eigenstate and epr principles, one can prove that the answer to the last question is affirmative: *Any infinite repetition of the experiment measuring a quantum value indefinite observable generates an uncomputable infinite sequence $x_1x_2\dots$: no PRNG has this randomness property.*

A stronger result is true. Informally, a sequence \mathbf{x} is bi-immune if no algorithm can generate infinitely many correct values of its elements (pairs, (i, x_i)). Formally, a sequence $\mathbf{x} \in A_b^\omega$ ($b \geq 2$) is *bi-immune* if there is no partially computable function φ from \mathbb{N} to A_b having an infinite domain $\text{dom}(\varphi)$ with the property that $\varphi(i) = x_i$ for all $i \in \text{dom}(\varphi)$ [12].

Theorem 2 ([1, 8]). *Assume the Eigenstate and epr principles. An infinite repetition of the experiment measuring a quantum value indefinite observable in \mathbb{C}^b always generates a b -bi-immune sequence $\mathbf{x} \in A_2^\omega$, for every $b \geq 2$.*

Theorem 3 ([8]). *Assume the epr and Eigenstate principles. Let \mathbf{x} be an infinite sequence obtained by measuring a quantum value indefinite observable in \mathbb{C}^b in an infi-*

¹The motivation comes from Einstein, Podolsky and Rosen’s definition of *physical reality* [26, p. 777].

nite repetition of the experiment E . Then, no single bit x_i can be predicted.

In particular, no single digit of every sequence $\mathbf{x} \in A_3^\omega$ generated by the 3D-QRNG can be algorithmically predicted.

The following simple morphism $\varphi: A_3 \rightarrow A_2$ transforms a ternary sequence into a binary sequence:

$$\varphi(a) = \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{if } a = 1, \\ 0 & \text{if } a = 2, \end{cases} \quad (1)$$

, which can be extended sequentially for strings, $\mathbf{y}(n) = \varphi(\mathbf{x}(n)) = \varphi(x_1)\varphi(x_2) \dots \varphi(x_n)$ and sequences $\mathbf{y} = \varphi(\mathbf{x}) = \varphi(x_1)\varphi(x_2) \dots \varphi(x_n) \dots$. This transformation preserves 2-bimmunity:

Theorem 4 ([8]). *Assume the epr and Eigenstate principles. Let $\mathbf{y} = \varphi(\mathbf{x})$, where $\mathbf{x} \in A_3^\omega$ is a ternary sequence generated by the 3D-QRNG and φ is the alphabetic morphism defined in (1). Then, no single bit of $\mathbf{y} \in A_2^\omega$ can be predicted.*

These results have been used to design the following quantum operators of the 3D-QRNG. These 3D-QRNGs operate in a succession of events of the form “preparation, measurement, reset”, iterated indefinitely many times in an algorithmic fashion [1]. The first 3D-QRNG was designed in [1], realized in [37] and analysed in [2]. While the analysis failed to observe a strong advantage of the quantum random sequences due to incomputability, it has motivated the improvement in [8], in which the problematic probability zero branch $S_x = 0$ in Figure 1.

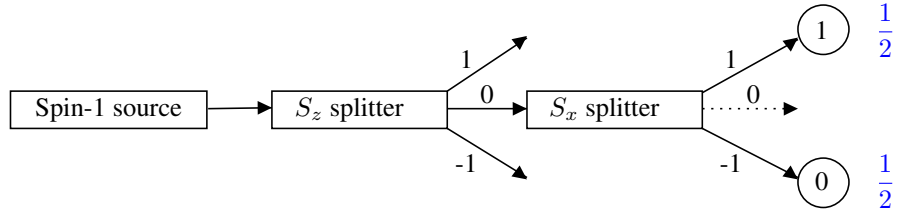


Figure 1: QRNG setup proposed in [1]; the values $\frac{1}{2}, \frac{1}{2}$ (in blue) correspond to the outcome probabilities

The next 3D-QRNG is presented in Figure 2. The unitary matrix U_x corresponding to the spin state operator S_x is

$$U_x = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}.$$

As U_x can be decomposed into two-dimensional transformations [18]

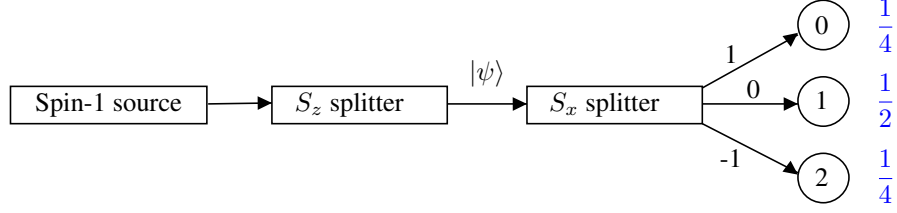


Figure 2: Blueprint for a new QRNG; the values $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ (in blue) correspond to the outcome probabilities of setups prepared in the state $|\psi\rangle = |\pm 1\rangle$

$$U_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & -i \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} & 0 \\ i\sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{3}}{2} & 0 & -\frac{i}{2} \\ 0 & 1 & 0 \\ \frac{i}{2} & 0 & -\frac{\sqrt{3}}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \\ 0 & i\sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} \end{pmatrix}.$$

a physical realisation of the unitary operator by a lossless beam splitter [47, 63] was obtained; the new outcome probabilities are $1/4, 1/2, 1/4$.

3. 3D-QRNG – Physical Realisation

To realise the protocols shown in Figs. 1,2 we used a standard superconducting transmon system [37]. The transmon has a weakly anharmonic multi-level structure [32], and its three lowest energy eigenstates $|0\rangle, |1\rangle$ and $|2\rangle$ can be used as the logical states of a qutrit.

To implement the protocol shown in Fig. 1 we followed the recipe from [37] where the eigenstates of the S_z operator are mapped to the states of the qutrit as follows

$$\{|z, -1\rangle, |z, 0\rangle, |z, +1\rangle\} \rightarrow \{|2\rangle, |0\rangle, |1\rangle\}. \quad (2)$$

This mapping provided an advantage of preparing $|z, 0\rangle$ state by cooling down the transmon to the base temperature of a dilution refrigerator (~ 20 mK).

To perform an arbitrary rotation of the qutrit quantum state $R_n^{i,i+1}(\phi)$ we applied microwave pulses resonant to the $|0\rangle \leftrightarrow |1\rangle$ or $|1\rangle \leftrightarrow |2\rangle$ transition frequencies, respectively. Two rotations $R_y^{12}(\pi) \cdot R_y^{01}(\pi/2)$ of the state before the dispersive measurement were used to engineer a measurement in the eigenbasis of S_x . The resulting measurement outcomes of the transmon energy eigenstates were mapped to the following outcomes of the measurement of S_x operator: $\{|0\rangle, |1\rangle, |2\rangle\} \rightarrow \{|x, +1\rangle, |x, -1\rangle, |x, 0\rangle\}$.

To implement the protocol shown in Fig. 2, we used a slightly different encoding:

$$\{|z, -1\rangle, |z, 0\rangle, |z, +1\rangle\} \rightarrow \{|1\rangle, |2\rangle, |0\rangle\}. \quad (3)$$

In this case, the state $|z, +1\rangle$ was prepared by cooling the transmon. The following measurement in the eigenbasis of S_x was engineered by applying the same rotations

$R_y^{01}(\pi/2) \cdot R_y^{12}(\pi/2)$ before the dispersive measurements. The measurement outcomes of the transmon were then mapped to the following outcomes of the measurement of S_x operator: $\{|0\rangle, |1\rangle, |2\rangle\} \rightarrow \{|x, 0\rangle, |x, -1\rangle, |x, +1\rangle\}$.

To measure the transmon, we used the standard dispersive readout scheme where the transmon is capacitively coupled to a co-planar waveguide resonator. The difference between the frequency of the resonator ($f_r = 7.63$ GHz) and the $|0\rangle \leftrightarrow |1\rangle$ ($f_{01} = 5.49$ GHz) and $|1\rangle \leftrightarrow |2\rangle$ ($f_{12} = 5.16$ GHz) transitions of the transmon was designed to be much larger than the qubit-resonator coupling to ensure that the system is in the dispersive regime. In this regime, the frequency of the resonator depended on the states of the transmon and underwent shifts of -8.5 MHz or -15.5 MHz when the transmon was excited in $|1\rangle$ or $|2\rangle$ states, relative to f_r when the transmon was prepared in its ground state $|0\rangle$ [32]. We used a Josephson parametric amplifier to distinguish between three different transmon states with high fidelity. In addition, we set the readout pulse frequency close to the cavity frequency corresponding to the $|1\rangle$ state of the qutrit, which allowed the three possible qutrit states to be well separated on the I-Q plane for the time-integrated signal measured with the heterodyne detection scheme. The readout frequency was then fine-tuned to maximise the three-level readout fidelity. The measurement response was classified using a convolutional neural network (CNN) to increase the readout fidelity further, as described in [43].

The procedure used to generate the random numbers required an initial calibration procedure typical for circuit quantum electrodynamics setups. This involved calibration of f_r , f_{01} and the $R_y^{01}(\pi)$ and $R_y^{01}(\pi/2)$ pulses. Two $R_y^{01}(\pi/2)$ pulses were used to fine-tune f_{01} using a Ramsey measurement. The $R_y^{01}(\pi)$ and $R_y^{01}(\pi/2)$ pulses were then fine-tuned with repeated pulses. A similar procedure was followed to calibrate for f_{12} and the $R_y^{12}(\pi)$ and $R_y^{12}(\pi/2)$ pulses.

After initial calibrations, we optimised the readout frequency of a single-shot readout using the Josephson parametric amplifier. The CNN is then trained for 50 cycles using 1024 measurements of the readout resonator after preparing each of the three states, $|0\rangle, |1\rangle$ and $|2\rangle$ as described in [43].

The procedure so far involved repeated measurements where the transmon was reset to $|0\rangle$ state by waiting $35 \mu\text{s}$ to reach thermal equilibrium (at a decay rate of 250 kHz). We used an active reset protocol described in [40] to increase the experiment cycle time. This involved a *reset pulse* to transfer the $|2\rangle$ state population to the readout resonator and let it decay much faster (at a decay rate of 4 MHz). An $R_y^{12}(\pi)$ pulse is then used to transfer the unwanted $|1\rangle$ state population to the $|2\rangle$ state, and the reset pulse was used again to transfer $|2\rangle$ state population to the readout resonator. The $R_y^{12}(\pi)$ (40 ns), reset pulse (370 ns), and a wait time (50 ns) for the readout resonator to decay were used four times in series to ensure the transmon is in the ground state, taking 1.84 μs in total. The reset time, the preparation pulses for the protocol and the measurement pulse time amounted to 3.2 μs , corresponding to a rate of 312.5 kHz. To ensure robust generation of 100 Gbit of random numbers we used the procedure in Section 4.

4. Data Generation

The quantum random numbers have been generated using the procedure in Algorithm 1. The algorithm involves intermittent checks of the CNN without a reset, if necessary, retraining the CNN and re-calibrating the transmon according to Algorithm 2.

Three types of errors could appear: initialisation errors, errors of the control pulses, and measurement errors. As the initialisation and control errors are calibrated to be kept within $< 1\%$, the measurement error was the dominant error: this is due to the relaxation of the higher excited states of the qutrit to the lower energy states during the readout time. The typical assignment fidelities have been 95%, 88%, and 78% for the ground, first and second excited states, respectively. All the fidelities have been continuously monitored during random number generation, and a drop in the value of the average assignment fidelity was used to trigger the re-calibration of the protocol (see Algorithm 1).

Algorithm 1 Generation

```
1: procedure RUNINDEX
2:   if files exist then
3:      $r \leftarrow 1 + \text{last } random\_xxx.rbf \text{ file number}$ 
4:   else
5:     return  $r \leftarrow 0$ 
6:   end if
7:   return  $r$ 
8: end procedure
9:  $T_{\text{rep}} \leftarrow 40 \mu\text{s}$ 
10: Prepare  $|0\rangle, |1\rangle$  and  $|2\rangle$  ▷ Cyclically for each repetition
11: Create convolutional neural network (CNN)
12: Train CNN for 50 training cycles
13:  $f \leftarrow \text{measurement accuracy}$  ▷ Assignment fidelity as defined in [43]
14:  $c \leftarrow 0$  ▷ Calibration counter used to terminate
15:  $l \leftarrow 0$  ▷ Low  $f$  counter used to calibrate
16:  $r \leftarrow \text{RUNINDEX}$ 
17: while  $r < 750$  do
18:   while  $f < 0.86$  do
19:     if  $l > 20$  then
20:       if  $c > 5$  then
21:         ERROR ▷ Calibrated 5 times already. Failed
22:       end if
23:       CALIBRATE
24:        $c \leftarrow c + 1$ 
25:        $l \leftarrow 0$ 
26:     end if
27:      $l \leftarrow l + 1$ 
28:     Train CNN for 20 more training cycles
29:      $f \leftarrow \text{measurement accuracy}$ 
30:   end while
31:    $T_{\text{rep}} \leftarrow 3.2 \mu\text{s}$ 
32:   Program protocol pulses
33:   Measure  $2^{26}$  repetitions
34:   Store measurements in  $random\_r.rbf$ 
35:    $T_{\text{rep}} \leftarrow 40 \mu\text{s}$ 
36: end while
```

Algorithm 2 Calibration

```
1: procedure CALIBRATE ▷ Calibrates the transmon preparation and readout
2:    $T_{\text{rep}} \leftarrow 40 \mu\text{s}$ 
3:   set measurement frequency to  $f_r$ 
4:   set previously calibrated settings
5:   Ramsey frequency calibration for  $f_{01}$ 
6:   Calibrate  $R_y^{01}(\pi)$  and  $R_y^{01}(\pi/2)$  pulses
7:   Ramsey frequency calibration for  $f_{12}$ 
8:   Calibrate  $R_y^{12}(\pi)$  and  $R_y^{12}(\pi/2)$  pulses
9:   Calibrate reset pulse frequency
10:  set measurement frequency to  $f_r - 9 \text{ MHz}$ 
11:  Create convolutional neural network (CNN)
12:  Train CNN for 50 training cycles
13: end procedure
```

5. Testing Incomputability

In this section, we present an empirical method to show the incomputability of the outputs generated in Section 3.

5.1. Why do we need testing?

Why should we be interested in answering the above question? After all, incomputability is established by mathematical proof, so why would we need experimental corroboration, a weaker argument? An example is a random number generator certified (by a mathematical proof) to always produce an incomputable infinite sequence of random bits. Indeed, the mathematical proof certifying incomputability is part of a mathematical model which uses certain physical assumptions; its veracity rests on those assumptions. The fact that each assumption is reasonable does not automatically guarantee that the set of assumptions is also reasonable globally. Experimental testing is essential not only for corroborating the conclusion of the proof but also for supporting the adequacy of the model. Furthermore, thorough testing allows one to detect any issues with assumptions made in the theoretical analysis of a device or its practical deployment.

Can we test incomputability with a statistical test, that is, with a method of statistical inference, to decide whether the data at hand sufficiently supports a particular hypothesis? The answer is *negative*. Intuitively, this is a consequence of the “asymptotic” nature of the notion of computability and its negation: *finite variations do not change them*. For example, if the sequence $x_1x_2 \dots x_n \dots$ is computable (incomputable), then the sequences $y_1y_2 \dots y_mx_1x_2 \dots x_n \dots$ and $x_kx_{k+1} \dots x_m \dots$ are also computable (incomputable) for every string $y_1y_2 \dots y_m$ and positive integer k . For example, the Champernowne binary sequence [17]

0, 1, 00, 01, 10, 11, 000, . . .

obtained by concatenating all binary strings in shortlex order.² This sequence is computable and *normal*, i.e. its digits are uniformly distributed: all digits are equally likely, all pairs of digits are equally likely, all triplets of digits are equally likely, and so on. Normality is a “symptom” of randomness, and computability is a “symptom” of non-randomness. The Champernown sequence shows that these symptoms can be compatible; no statistical test can detect its computability, hence non-randomness.

Does this mean that incomputability cannot be “experimentally tested”? Of course, no. In what follows, we will describe such a test used in assessing the quality of outputs of quantum random generators, [14, 2].

5.2. Theory

We continue with a topic apparently unrelated to the question discussed in this section: testing of primality of positive integers. Primality is considered computationally *easy* because there exist polynomial algorithms in the size of the input to solve it; the first such algorithm was proposed in 2004 [7]. However, every known primality polynomial algorithm is “practically slow”, so probabilistic algorithms³ are instead used [52].⁴

The practical failure of polynomial primality tests motivated the search for probabilistic algorithms for primality [41, 46, 49, 50, 52, 52]. To test the primality of a positive integer n , the Solovay-Strassen primality test generates the first k natural numbers uniformly distributed between 1 and $n - 1$, inclusive, and, for each $i \in \{i_1, \dots, i_k\}$ checks “quickly” the validity of a predicate $W(i, n)$ based on Euler’s criterion (called the Solovay-Strassen predicate). If $W(i, n)$ is true then “ i is a witness of n ’s compositeness”; hence n is certainly not prime. Otherwise, the test is inconclusive. In this case, the probability that n is prime is greater than $1 - 2^{-k}$. This result is based on the fact that *at least half* the i ’s between 1 and $n - 1$ satisfy $W(i, n)$ if n is composite, and *none* of them satisfy $W(i, n)$ if n is prime [51].

In detail, we first define the Solovay-Strassen predicate $W(i, n)$ by

$$\left(\frac{i}{n}\right) i^{(n-1)/2} \not\equiv 1 \pmod{n},$$

where $\left(\frac{i}{n}\right)$ is the Jacobi symbol⁵ with $i \in \mathbb{N}, i < n - 1$.

²Strings are first sorted by increasing length, and strings of the same length are sorted into lexicographical order: 0, 1; 00, 01, 10, 11; 000, 001, . . . 111; . . .

³Currently the best runs in time $O((\log n)^6)$.

⁴In contrast, factorisation of positive integers is “thought”, but not proved, to be a computationally *difficult* problem. Currently, one cannot factorise a positive integer of 500 decimal digits that is the product of two randomly chosen prime numbers. This fact is exploited in the RSA cryptosystem implementing public-key cryptography [48].

⁵If the prime factorisation of the odd number n is $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then $\left(\frac{i}{n}\right) =$

If $i \geq 2$ and $W(i, n)$ is true, we say that i is an *Euler witness* (*E-witness*). If $n > 3$ is an odd composite, and $W(i, n)$ is false for $i \geq 1$, we say n is an *Euler pseudo-prime* for the base i or that i is an *Euler liar* (*E-liar*) for the Solovay-Strassen primality test. In particular, the set $L_{ss}(n)$ of *E-liars* has at most $\frac{\phi(n)}{2}$ elements. Thus, the probability of sampling an *E-liar* when performing the Solovay Strassen test is given by $\beta_n = |L_{ss}(n)|/(n-1)$

The size of $L_{ss}(n)$ varies for different odd composite numbers. Consider the Carmichael numbers, that is, composite positive integers n satisfying the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all integers b relatively prime to n . The largest β_n is found in a subset of Carmichael numbers with $\beta_n = \frac{1}{2}$. A Carmichael number passes a Fermat primality test [20, Section 31.8] to every base relatively prime to the number, but few of them pass the Solovay-Strassen test. Increasingly Carmichael numbers become “rare”.⁶

Consider $s = s_0 \dots s_{m-1}$ a binary string (of length m) and n an integer greater than 2. Let k be the smallest integer such that $(n-1)^{k+1} > 2^m - 1$; we can thus rewrite the number whose binary representation is s into base $n-1$ and obtain the unique string $d_k d_{k-1} \dots d_0$ over the alphabet $\{0, 1, \dots, n-2\}$, that is,

$$\sum_{i=0}^k d_i (n-1)^i = \sum_{t=0}^{m-1} s_t 2^t.$$

The predicate $Z(s, n)$ is defined by

$$Z(s, n) = \neg W(1 + d_0, n) \wedge \dots \wedge \neg W(1 + d_{k-1}, n), \quad (4)$$

where W is the Solovay-Strassen predicate.

The digits of s (rewritten in base $n-1$) are used to define the Solovay Strassen predicates. If n is a pseudo-prime for all the bases from s used to construct these predicates, we say that s is a Z -*liar*.

A string s is c -random if $K(s) \geq |s| - c$; $|s|$ is the string length and K is the Kolmogorov complexity [13].

Chaitin-Schwartz Theorem. [16] *For all sufficiently large c , if s is a c -random string of length $(l + 2c)$ and n is an integer whose binary representation is l bits long, then $Z(s, n)$ is true if and only if n is prime.*

This result cannot be used to de-randomise⁷ Solovay-Strassen probabilistic algorithm because the set of c -random strings is incomputable.⁸ However, the result can be used to model strings from different random number generators to test the quality of long binary strings by comparing their behaviour. In particular, we look at the number of Z -liars found by each generator.

$$\left(\frac{i}{p_1}\right)^{a_1} \left(\frac{i}{p_2}\right)^{a_2} \dots \left(\frac{i}{p_k}\right)^{a_k}.$$

⁶There are 1,401,644 Carmichael numbers in the interval $[1, 10^{18}]$.

⁷That is, to transform the probabilistic algorithm into an equivalent deterministic algorithm.

⁸In fact, highly incomputable [13]; no infinite set of c -random is computable.

5.3. Experimental analysis

Standard statistical tests of randomness focus on properties of the distribution of bits or bit strings within sequences, failing to distinguish between pseudo-random number generators and quantum random number generators. To address this issue, in [2], the ability of random strings to de-randomise the Solovay-Strassen probabilistic test of primality was used to compare the algorithmic randomness of strings generated by a QRNG and those produced by different PRNGs. Despite leading to mostly inconclusive results, the tests conducted showed some advantages offered by a 3D-QRNG against PRNGs with respect to the randomness of its outputs.

The following test, called the fourth Chaitin-Schwartz-Solovay-Strassen test (CSS4) in [2], showed the highest potential for distinguishing between sources of random strings. Recall that the crucial fact is that the set of c -random strings is (highly) *incomputable*.

We construct the Chaitin-Schwartz predicate $Z(s, n)$ from (4) and generate a pool of Solovay-Strassen predicates composed of the digits s in base $n - 1$. Then, we fix $c = l - 1$ where l is the l -bit binary representation of n and sample s from chunks of $l(l + 2c)$ bits in order to look for Z -liars generated by a set of bases for the predicates extracted from the string s .

In [2], Carmichael numbers were used in the majority of the tests. However, despite Carmichael numbers having a larger $L_{ss}(n)$, it is difficult to find Z -liars due to the length of their binary representation. For example, for the smallest Carmichael number more than 70×2^{32} bits would need to be read to find a Z -liar since the Solovay-Strassen test guarantees a predicate is true with a probability of at least one-half when n is a composite number. For smaller numbers we expect see to a larger number of Z -liars. Thus, for this test, only odd composite numbers less than 50 were used for each round, and the process was repeatedly parsed through each string with an incremental bit offset.

Recently in [31], a similar approach was taken by applying these tests to a different set of PRNGs and two different QRNGs with a larger set of numbers; each string tested had a length of 2^{26} . Once again, the QRNGs showed no clear advantage over the PRNGs. Moreover, the difficulty of finding Z -liars led to a similar limitation in terms of numbers tested; Z -liars were only observed for composites $n \leq 25$. Still, an essential characteristic of this test was confirmed: its sensitivity to the size of the pool of unique bases extracted from the random strings. No Z -liars were recorded when a repetitive structure generated by their sampling process was present. For this reason, we have a variation of this test was performed.

We tested two PRNGs and a QRNG: the Python3 Mersenne Twister-based generator, the hashing function SHA3, considered a “cryptographically secure PRNG” and the 3D-QRNG described in this paper.

Since the number of Solovay-Strassen tests increases with longer binary representations, the probability of observing a Z -liar becomes smaller, so a large pool of unique bases was required to detect a significant number of Z -liars [2]. Thus, we prepared ten

Composite number tested	9	15	21	25	27	33	35	39	45	49
sha3	265.6	60.3	0	0.2	0	0	0	0	0	0
python3	260.1	58	0	0.3	0	0	0	0	0	0
qutrits	536.4	131.9	0	0.2	0	0	0	0	0	0

Table 1: Average number of *Z-liars* sampled by composite number tested (over 10 strings of length 2^{32})

sets of strings of size 2^{32} for each generator and applied the shifting process described in [2] for the test. The average number of *Z-liars* over the composite numbers less than 50 was taken as the metric. Despite only detecting *Z-liars* for composites up to 25, there was a noticeable difference between sources for the numbers 9 and 15. For these numbers, from our predicate construction, we have that a minimum of 40×2^{13} bits and 40×2^{10} bits are needed for a *c*-random string to have a chance of finding a *Z-liar*; see Table 1.

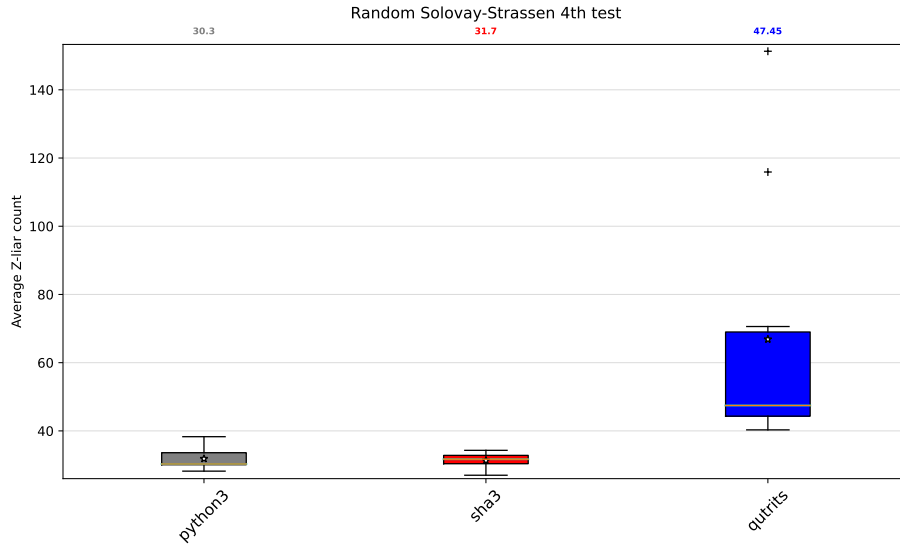


Figure 3: Fourth Chaitin-Schwartz-Solovay-Strassen test: distribution of the average *Z-liar* counts for all odd composite numbers less than 50

The occurrence of patterns in long enough sequences of random events is inevitable. Since a lower quality of randomness increases the rate at which this occurs, the gap between the number of unique bases extractable between RNGs with different qualities of randomness widens. Thus, given long enough strings, we can observe this behaviour. Since many unique bases are required to increase the likelihood of finding *Z-liars*, from Figure 1, we see the advantage offered by a 3D-QRNG generator over other alternative sources of randomness; see Fig. 3.

In order to analyse the statistical significance of these results, we conducted the non-parametric and distribution-free two-sample Kolmogorov–Smirnov test. This test iden-

	sha3	qutrits
python3	0.9780	0.0047
sha3		0.0047

Table 2: Kolmogorov-Smirnov test p -values for the fourth Chaitin-Schwartz-Solovay-Strassen test with the Z-liar count metric

tifies if two datasets differ significantly without any prior assumption about an underlying distribution. To this end, we say that the difference between two datasets is statistically significant if the p -value obtained through this test is less than 0.005. This critical p -value is chosen to reduce the chance of false positives as well as allow us to provide a direct comparison with results from [2]; see Table 2.

We note that there is a significant difference between the 3D-QRNG qutrits and the PRNGs. A similar behaviour was revealed in [2], where despite the non-conclusive results of the fourth Chaitin-Schwartz-Solovay-Strassen test, the Kolmogorov-Smirnoff test showed that the difference between a 3D-QRNG and the other PRNGs is statistically relevant. The outcomes of the fourth Chaitin-Schwartz-Solovay-Strassen test presented here show a stronger advantage of 3D-QRNGs over PRNGs.

6. Conclusions

This article uses a located form of the Kochen-Specker Theorem to derive a physical realisation of a class of 3D-QRNGs by means of a superconducting transmon. The sequences produced by these 3D-QRNGs are strongly uncomputable, a property that no other QRNG provides to date. Furthermore, we have used a non-statistical randomness test to probe experimentally the uncomputability of its generated long strings: for the first time, a provable advantage over the best PRNGs was found. This result has been achieved by using the Chaitin-Schwartz Theorem to probe the “usefulness” of generated quantum random bits, a form of Einstein’s justification.

These results highlight the real effects of uncomputability in quantum systems and complement the theoretical certification via value indefiniteness of the class of QRNGs implemented. Furthermore, the experimental results confirm and complement uncomputability and, quite significantly, the choice of physical assumptions in the theoretical part.

Finally, there is a strong motivation for developing alternative tests capable of probing at algorithmic properties of randomness that better suit a wide range of applications where the quality of randomness needs to be assessed quickly or dynamically.

References

- [1] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil. Strong Kochen-Specker theorem and uncomputability of quantum randomness. *Physical Review A*, 86(062109), Dec 2012.

- [2] A. A. Abbott, C. S. Calude, M. J. Dinneen, and N. Huang. Experimentally probing the algorithmic randomness and incomputability of quantum randomness. *Physica Scripta*, 94:045103, 2019.
- [3] A. A. Abbott, C. S. Calude, and K. Svozil. Value-indefinite observables are almost everywhere. *Physical Review A*, 89(032109), 2013.
- [4] A. A. Abbott, C. S. Calude, and K. Svozil. A quantum random number generator certified by value indefiniteness. *Mathematical Structures in Computer Science*, 24:e240303, 6 2014.
- [5] A. A. Abbott, C. S. Calude, and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6(4):773–789, 2015.
- [6] A. A. Abbott, C. S. Calude, and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness. *Journal of Mathematical Physics*, 56, 102201, <http://dx.doi.org/10.1063/1.4931658>, Oct 2015.
- [7] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.
- [8] J. M. Agüero Trejo and C. S. Calude. A new quantum random number generator certified by value indefiniteness. *Theoretical Computer Science*, 862:3–13, Mar. 2021.
- [9] J. M. Agüero Trejo and C. S. Calude. Photonic ternary quantum random number generators. *Proc. R. Soc. A*, 479:1–16, 2023.
- [10] J. Bausch, T. S. Cubitt, A. Lucia, and D. Perez-Garcia. Undecidability of the spectral gap in one dimension. *Phys. Rev. X*, 10:031038, Aug 2020.
- [11] R. Bernardo-Gavito, I. E. Bagci, J. Roberts, J. Sexton, B. Astbury, H. Shokeir, T. McGrath, Y. J. Noori, C. S. Woodhead, M. Missous, U. Roedig, and R. J. Young. Extracting random numbers from quantum tunnelling through a single diode. *Scientific Reports*, 7(1):17879, 2017.
- [12] L. Bienvenu, A. R. Day, and R. Hölzl. From bi-immunity to absolute undecidability. *J. Symbolic Logic*, 78(4):1218–1228, 12 2013.
- [13] C. Calude. *Information and Randomness—An Algorithmic Perspective*. Springer, Berlin, 2002 (2nd ed.).
- [14] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil. Experimental evidence of quantum randomness incomputability. *Physical Review A*, 82, 022102:1–8, 2010.
- [15] C. S. Calude and K. Svozil. Quantum randomness and value indefiniteness. *Advanced Science Letters*, 1(2):165–168, 2008. eprint arXiv:quant-ph/0611029.

- [16] G. J. Chaitin and J. T. Schwartz. A note on Monte Carlo primality tests and algorithmic information theory. *Communications on Pure and Applied Mathematics*, 31(4):521–527, 1978.
- [17] D. G. Champernowne. The construction of decimals normal in the scale of ten. *The Journal of London Mathematical Society*, 8:254–260, 1933.
- [18] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, Dec 2016.
- [19] B. S. Cooper and P. Odifreddi. Incomputability in nature. In S. B. Cooper and S. S. Goncharov, editors, *Computability and Models: Perspectives East and West*, pages 137–160. Plenum Press, New York, 2003.
- [20] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. The MIT Press, 3rd edition edition, 2009.
- [21] J. F. Costa. Incomputability at the foundations of physics (A study in the philosophy of science). *Journal of Logic and Computation*, 23(6):1225–1248, 2013.
- [22] T. S. Cubitt, D. Perez-Garcia, and M. M. Wolf. Undecidability of the spectral gap. *Nature*, 528(7581):207–211, 2015.
- [23] N. C. A. da Costa and F. A. Doria. Undecidability and incompleteness in classical mechanics. *International Journal of Theoretical Physics*, 30:1041–1073, Aug. 1991.
- [24] F. Diacu. The solution of the n-body problem. *The Mathematical Intelligencer*, 18(3):66–70, 1996.
- [25] A. Einstein. Physics and reality. *Journal of the Franklin Institute*, 221(3):349–382, 1936.
- [26] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, May 1935.
- [27] N. Gisin. Indeterminism in physics and intuitionistic mathematics. *Synthese*, 199(13345–13371), 2021.
- [28] ID Quantique SA. *Random Number Generation – White Paper: What is the Q in QRNG?* idQuantique, Geneva, Switzerland, May 2020.
- [29] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71:1675–1680, 2000.
- [30] I. Kanter. Undecidability principle and the uncertainty principle even for classical systems. *Physical Review Letters*, 64:332–335, 1990.

- [31] J. T. Kavulich, B. P. Van Deren, and M. Schlosshauer. Searching for evidence of algorithmic randomness and incomputability in the output of quantum random number generators. *Physics Letters A*, page 127032, 2020.
- [32] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Charge-insensitive qubit design derived from the cooper pair box. *Phys. Rev. A*, 76:042319, Oct 2007.
- [33] S. B. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967. Reprinted in E. Specker. *Selecta*. Birkhäuser Verlag, Basel, 1990.
- [34] K. W. F. Kohlrausch. *Der experimentelle Beweis für den statistischen Charakter des radioaktiven Zerfallsgesetzes*, pages 192–212. Springer, Berlin, Heidelberg, 1926.
- [35] H. Kragh. Subatomic determinism and causal models of radioactive decay, 1903–1923. RePoSS: Research Publications on Science Studies 5. Department of Science Studies, University of Aarhus, November 2009.
- [36] G. Kreisel. A notion of mechanistic theory. *Synthese*, 29:11–26, 1974.
- [37] A. Kulikov, M. Jerger, A. Potočník, A. Wallraff, and A. Fedorov. Realization of a quantum random generator certified with the Kochen-Specker theorem. *Phys. Rev. Lett.*, 119:240501, Dec 2017.
- [38] S. Lloyd. Uncomputability and physical law. In S. B. Cooper and M. I. Soskova, editors, *The Incomputable: Journeys Beyond the Turing Barrier*, Theory and Applications of Computability, pages 95–104. Springer International Publishing, 2017.
- [39] G. Longo. Incomputability in physics. In F. Ferreira, B. Löwe, E. Mayordomo, and L. Mendes Gomes, editors, *Programs, Proofs, Processes*, pages 276–285, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
- [40] P. Magnard, P. Kurpiers, B. Royer, T. Walter, J.-C. Besse, S. Gasparinetti, M. Pechal, J. Heinsoo, S. Storz, A. Blais, and A. Wallraff. Fast and unconditional all-microwave reset of a superconducting qubit. *Phys. Rev. Lett.*, 121:060502, Aug 2018.
- [41] G. Miller. Riemann’s hypothesis and tests for primality. *J. Comp. Syst. Sci.*, 13:300–317, 1976.
- [42] C. D. Moore. Unpredictability and undecidability in dynamical systems. *Physical Review Letters*, 64:2354–2357, 1990. Cf. Ch. Bennett, *Nature*, **346**, 606 (1990).
- [43] R. Navarathna, T. Jones, T. Moghaddam, A. Kulikov, R. Beriwal, M. Jerger, P. Pakkiam, and A. Fedorov. Neural networks for on-the-fly single-shot state classification. *Applied Physics Letters*, 119(11):114003, Sept. 2021.

- [44] H. Poincaré. *Wissenschaft und Hypothese*. Teubner, Leipzig, 1914.
- [45] M. B. Pour-El and J. I. Richards. *Computability in Analysis and Physics*. Springer, Berlin, 1989.
- [46] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Th.*, 12,:128–138, 1980.
- [47] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61, 1994.
- [48] H. Riesel. *Prime Numbers and Computer Methods for Factorization*, chapter Classical Methods of Factorization, pages 141–172. Birkhäuser Boston, Boston, MA, 2012.
- [49] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6(1):84–85, 1977.
- [50] R. Solovay and V. Strassen. Erratum: A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 7(1):118, 1978.
- [51] R. M. Solovay. On random r.e. sets. In A. I. Arruda, N. C. A. da Costa, and R. Chuaqui, editors, *Non-Classical Logics, Model Theory, and Computability*, pages 283–307. North-Holland, Amsterdam, 1977.
- [52] A. Stiglic. *Encyclopedia of Cryptography and Security*, chapter Probabilistic Primality Test, pages 980–980. Springer US, Boston, MA, 2011.
- [53] K. F. Sundman. Memoire sur le problème de trois corps. *Acta Mathematica*, 36:105–179, 1912.
- [54] P. Suppes. The transcendental character of determinism. *Midwest Studies In Philosophy*, 18(1):242–257, 1993.
- [55] K. Svozil. The quantum coin toss – testing microphysical undecidability. *Physics Letters A*, 143:433–437, 1990.
- [56] K. Svozil. *Randomness & Undecidability in Physics*. World Scientific, Singapore, 1993.
- [57] K. Svozil. Omega and the time evolution of the n-body problem. In C. S. Calude, editor, *Randomness and Complexity, from Leibniz to Chaitin*, pages 231–236, Singapore, 2007. World Scientific. eprint arXiv:physics/0703031.
- [58] K. Svozil. *Physical (A)Causality*, volume 192 of *Fundamental Theories of Physics*. Springer International Publishing, Cham, Heidelberg, New York, Dordrecht, London, 2018.
- [59] Q. D. Wang. The global solution of the n -body problem. *Celestial Mechanics*, 50:73–88, 1991.

- [60] Q. D. Wang. Power series solutions and integral manifold of the n-body problem. *Regular & Chaotic Dynamics*, 6(4):433–442, 2001.
- [61] C. Weierstrass, C. Hermite, and G. Mittag-Leffler. Mittheilung, einen von König Oscar II gestifteten mathematischen Preis betreffend. Communication sur un prix de mathématiques fondé par le roi Oscar II. *Acta Mathematica*, 7(1):I–VI, 1885.
- [62] S. Wolfram. Undecidability and intractability in theoretical physics. *Physical Review Letters*, 54(8):735–738, Feb 1985.
- [63] B. Yurke, S. L. McCall, and J. R. Klauder. SU(2) and SU(1,1) interferometers. *Physical Review A*, 33:4033–4054, 1986.
- [64] H. Zenil, editor. *Computable Universe: Understanding and Exploring Nature as Computation*. World Scientific, Singapore, 2013.