Mathematical undecidability and quantum randomness

Tomasz Paterek,[1,*] Johannes Kofler,[1,2] Robert Prevedel,[2] Peter Klimek,[2,†]
Markus Aspelmeyer,[1,2] Anton Zeilinger,[1,2] and Časlav Brukner[1,2]
[1]*Institut für Quantenoptik und Quanteninformation (IQOQI), Österreichische Akademie der Wissenschaften, Boltzmanngasse 3, 1090 Wien, Austria*
[2]*Fakultät für Physik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria*
(Dated: November 27, 2008)

We propose a new link between mathematical undecidability and quantum physics. We demonstrate that the states of elementary quantum systems are capable of encoding mathematical axioms and show that quantum measurements are capable of revealing whether a given proposition is decidable or not within the axiomatic system. Whenever a mathematical proposition is undecidable within the axioms encoded in the state, the measurement associated with the proposition gives random outcomes. Our results support the view that quantum randomness is irreducible and a manifestation of mathematical undecidability.

Whenever a proposition and a given set of axioms together contain more information than the axioms themselves, the proposition can neither be proved nor disproved from the axioms – it is mathematically undecidable [1, 2]. Here we propose a novel link between mathematical undecidability and quantum physics. We demonstrate that the states of elementary quantum systems are capable of encoding mathematical axioms. Quantum mechanics imposes an upper limit on how much information can be encoded in a quantum state [3, 4], thus limiting the information content of the set of axioms. We show that quantum measurements are capable of revealing whether a given proposition is decidable or not. Whenever a mathematical proposition is undecidable within the system of axioms encoded in the state, the measurement associated with the proposition gives random outcomes. This allows for an *experimental* test of mathematical undecidability by realizing in the laboratory both the actual quantum states and the required quantum measurements. (To illustrate these ideas, we conducted experiments using the polarization of photons.) Our results support the view that quantum randomness is irreducible [5, 6] and a manifestation of mathematical undecidability.

Any formal system is based on axioms, which are propositions that are defined to be true. A proposition is *logically independent* from a given set of axioms if it can neither be proved nor disproved from the axioms. If a proposition is independent from the axioms, neither the proposition itself nor its negation creates an inconsistency together with the axiomatic system.

In 1931, Gödel showed that arithmetic cannot be completed (without making it inconsistent by adding a wrong statement) [7, 8]. This implies that, keeping consistency and adding further and further axioms, one can always find new propositions that are logically independent from the (growing) axiomatic set. In the context of Gödel's incompleteness theorem, logically independent propositions are normally called *mathematically undecidable*. To name two famous examples: The so called "axiom of choice" is undecidable within the axioms of Zermelo-Fraenkel set theory, and the continuum hypothesis is undecidable within the Zermelo-Fraenkel set theory with the axiom of choice.

In this paper, we will consider mathematical undecidability in certain axiomatic systems which can be completed and which therefore are *not* subject to Gödel's incompleteness theorem. We will employ the notion that mathematical undecidability and logical independence are two expressions of the same fact, namely that a proposition can neither be proved nor disproved from the axioms. Take for example the axioms of (neutral) geometry and consider Euclid's "parallel postulate" as a proposition. In 1899, Hilbert showed that the parallel postulate is independent from the axioms [9]. Assuming the parallel postulate or its negation as an additional axiom, leads to *complete* and consistent Euclidean or Non-Euclidean geometries, respectively.

Intuitively, undecidable propositions contain entirely *new information* which cannot be reduced to the information in the axioms. This point of view led to the information-theoretical formulation of mathematical undecidability [1, 2]: Given a set of axioms that contains a certain amount of information, it is impossible to deduce the truth value of a proposition which, together with the axioms, contains more information than the set of axioms itself.

To give an example, consider Boolean functions of a single binary argument:

$$x \in \{0,1\} \;\rightarrow\; y = f(x) \in \{0,1\} \tag{1}$$

x	y_0	y_1	y_2	y_3
0	0	0	1	1
1	0	1	0	1

FIG. 1: The four Boolean functions $y = f(x)$ of a binary argument, i.e. $f(x) = 0, 1$ with $x = 0, 1$. The different functions are labeled by y_k with $k = 0, 1, 2, 3$.

There are four such functions, y_k ($k = 0, 1, 2, 3$), shown in Figure 1. We shall discuss the following (binary) propositions about their properties:

(A) "The value of $f(0)$ is '0', i.e. $f(0) = 0$."
(B) "The value of $f(1)$ is '0', i.e. $f(1) = 0$."

These two propositions are *independent*. Knowing the truth value of one of them does not allow to infer the truth value of the other. Ascribing truth values to both propositions requires two bits of information. If one postulates only proposition (A) to be true, i.e. if one chooses (A) as an 'axiom', then it is impossible to prove proposition (B) from (A). Having only axiom (A), i.e. only this one bit of information, there is *not enough information* to know also the truth value of (B). Hence, proposition (B) is *mathematically undecidable* within the system containing the single axiom (A). Another example of an undecidable proposition within the same axiomatic system is:

(C) "The function is constant, i.e. $f(0) = f(1)$."

Again, this statement can neither be proved nor disproved from the axiom (A) alone because (C) is independent of (A) as it involves $f(1)$.

We refer to such independent propositions to which one cannot simultaneously ascribe definite truth values – given a limited amount of information resources – as *logically complementary propositions*. Knowing the truth value of one of them precludes any knowledge about the others. Given the limitation of one bit of information encoded in the axiom, all three propositions (A), (B) and (C) are logically complementary to each other.

When the information content of the axioms and the number of independent propositions increase, more possibilities arise. Already the case of two bits as the information content is instructive. Consider two independent Boolean functions $f_1(x)$ and $f_2(x)$ of a binary argument. The two bits may be used to define properties of the individual functions or they may define joint features of the functions. An example of the first type is the following two-bit proposition:

(D) "The value of $f_1(0)$ is '0', i.e. $f_1(0) = 0$."
"The value of $f_2(1)$ is '0', i.e. $f_2(1) = 0$."

An example of the second type is:

(E) "The functions have the same values for argument '0', i.e. $f_1(0) = f_2(0)$."
"The functions have the same values for argument '1', i.e. $f_1(1) = f_2(1)$."

Both (D) and (E) consist of two elementary (binary) propositions. Their truth values are of the form of vectors with two components being the truth values of their elementary propositions. The propositions (D) and (E) are logically complementary. Given (E) as a two-bit axiom, all the *individual* function values remain undefined and thus one can determine neither of the two truth values of (D).

A qualitatively new aspect of multi-bit axioms is the existence of "partially" undecidable propositions, i.e. propositions that contain more than one elementary proposition and of which only some are undecidable. An example of such a partially undecidable proposition within the system consisting of the two-bit axiom (D) is:

(F) "The value of $f_1(0)$ is '0', i.e. $f_1(0) = 0$."
"The value of $f_2(0)$ is '0', i.e. $f_2(0) = 0$."

The first elementary proposition is the same as in (D) and thus it is definitely true. The impossibility to decide the second elementary proposition leads to partial undecidability of proposition (F). In a similar way, proposition (F) is partially undecidable within the axiomatic system of (E).

The discussion so far was purely *mathematical*. We have described finite axiomatic systems (of limited information content) using properties of Boolean functions. Now we show that the undecidability of mathematical propositions can be tested in quantum experiments. To this end we introduce a *physical* "black box" whose internal configuration encodes Boolean functions. The black box hence forms a bridge between mathematics and physics. Quantum systems enter it and the properties of the functions, i.e. the truth values of propositions, are written onto the quantum states of the systems. Finally, measurements performed on the systems extract information about the properties of the configuration of the black box and thus about the properties of the functions.

We begin with the simplest case of a qubit (e.g. a spin-$\frac{1}{2}$ particle or the polarization of a photon) entering the black box in a well-defined state and a single bit-to-bit function $f(x)$ encoded in the black box. Inside the black box two subsequent operations alter the state of the input qubit. The first operation encodes the value of $f(1)$ via application of $\hat{\sigma}_z^{f(1)}$, i.e. the Pauli z-operator taken to the power of $f(1)$. The second operation encodes $f(0)$ with $\hat{\sigma}_x^{f(0)}$, i.e. the Pauli x-operator taken to the power of $f(0)$. The total action of the black box is

$$\hat{U} = \hat{\sigma}_x^{f(0)}\,\hat{\sigma}_z^{f(1)}\,. \tag{2}$$

Consider the input qubit to be in one of the eigenstates of the Pauli operator $\mathrm{i}^{mn}\,\hat{\sigma}_x^m\,\hat{\sigma}_z^n$ (with i the imaginary unit). The three particular choices $(m,n) = (0,1)$, $(1,0)$, or $(1,1)$ correspond to the three Pauli operators along orthogonal directions (in the Bloch sphere) $\hat{\sigma}_z$, $\hat{\sigma}_x$, or $\hat{\sigma}_y = \mathrm{i}\,\hat{\sigma}_x\,\hat{\sigma}_z$, respectively. The measurements of these operators are quantum complementary: Given a system in an eigenstate of one of them, the results of the other measurements are totally random. The input density matrix reads

$$\hat{\rho} = \tfrac{1}{2}\left[\mathbb{1} + \lambda_{mn}\,\mathrm{i}^{mn}\,\hat{\sigma}_x^m\,\hat{\sigma}_z^n\right], \tag{3}$$

with $\lambda_{mn} = \pm 1$ and $\mathbb{1}$ the identity operator. It evolves under the action of the black box to

$$\hat{U}\hat{\rho}\,\hat{U}^\dagger = \tfrac{1}{2}\left[\mathbb{1} + \lambda_{mn}\,(-1)^{nf(0)+mf(1)}\,\mathrm{i}^{mn}\,\hat{\sigma}_x^m\,\hat{\sigma}_z^n\right]. \tag{4}$$

Depending on the value of $n\,f(0) + m\,f(1)$ (throughout the paper all sums are taken modulo 2), the state after the black box is either the same or orthogonal to the initial one. If one now performs a measurement in the basis of the initial state, (i.e. the eigenbasis of the operator $\mathrm{i}^{mn}\,\hat{\sigma}_x^m\,\hat{\sigma}_z^n$), the outcome reveals the value of $n\,f(0) + m\,f(1)$ and hence the measurement can be considered as *checking the truth value of the proposition*

(G) "$n\,f(0) + m\,f(1) = 0$."

It is crucial to note that each of the three quantum complementary measurements $\hat{\sigma}_z$, $\hat{\sigma}_x$, or $\hat{\sigma}_y$ – given the suitable initial state – reveals the truth value of one of the independent propositions (A), (B), or (C), respectively.

Independent of the initial state, we now identify the quantum measurement (m,n) with the question about the truth value of the corresponding mathematical proposition (G). Those states that give a definite (i.e. not random) outcome in the quantum measurement encode (G) or its negation as an axiom. For example, the two eigenstates of $\hat{\sigma}_z$ after the black box encode (A) or its negation as an axiom, and the $\hat{\sigma}_z$ measurement reveals the truth value of the proposition (A). This one bit is the maximal amount of information that can be encoded in a qubit [3, 4].

When a physical system prepared in an eigenstate of a Pauli operator is measured along complementary directions, the measurement outcomes are *random*. Correspondingly, the proposition identified with a complementary observable is *undecidable* within the one-bit axiom encoded in the measured state. For example, the measurement of $\hat{\sigma}_x$ on an eigenstate of $\hat{\sigma}_z$ gives random outcomes, and accordingly proposition (B) is undecidable within the one-bit axiom (A). This links mathematical undecidability and quantum randomness in complementary measurements. We propose that it is therefore possible to *experimentally* find out whether a proposition is decidable or not, as summarized in Figure 2.

In a single experimental run it is impossible to infer whether the outcome is definite or random and thus whether it stemmed from a decidable or undecidable proposition. Therefore, any quantum experiment revealing mathematical

Mathematics/Logic		Quantum Physics
Axioms of limited information content	↔	Quantum states
Boolean functions	↔	Unitary transformations
Question about proposition	↔	Quantum measurement
Decidability/Undecidability	↔	Definiteness/Randomness of outcomes

FIG. 2: The link between mathematical undecidability and quantum randomness.

undecidability requires many runs. (It can be shown that – given a certain level of noise – the probability to infer wrongly whether the proposition is decidable or not decays exponentially with the length of the outcome string.)

In order to further illustrate the developed theoretical concepts, we present in the Appendix the results of an experiment using the polarization degree of freedom of single photons as qubits. This experiment confirms that the decidability (undecidability) of propositions corresponds to a sequence of definite (random) outcomes of quantum measurements; see Figure 3 in the Appendix.

Generalizing the above reasoning to multiple qubits, we show in the following that *whenever* the proposition identified with a Pauli group measurement is decidable (within the axioms encoded into the qubits), the measurement outcome is definite, and whenever it is undecidable, the measurement outcome is random. Consider N black boxes, one for each qubit. They encode N Boolean functions $f_j(x)$ numbered by $j = 1, \dots, N$ by applying the operation

$$\hat{U}_N = \hat{\sigma}_x^{f_1(0)}\,\hat{\sigma}_z^{f_1(1)} \otimes \cdots \otimes \hat{\sigma}_x^{f_N(0)}\,\hat{\sigma}_z^{f_N(1)}\,. \tag{5}$$

The initial N-qubit state is chosen to be a particular one of the 2^N eigenstates of certain N *independent and mutually commuting* tensor products of Pauli operators, numbered by $p = 1, ..., N$:

$$\hat{\Omega}_p \equiv \mathrm{i}^{m_1(p)n_1(p)}\,\hat{\sigma}_x^{m_1(p)}\,\hat{\sigma}_z^{n_1(p)} \otimes \cdots \otimes \mathrm{i}^{m_N(p)n_N(p)}\,\hat{\sigma}_x^{m_N(p)}\,\hat{\sigma}_z^{n_N(p)}\,, \tag{6}$$

with $m_j(p), n_j(p) \in \{0, 1\}$. A broad family of such states is the family of stabilizer [11, 12] and graph states [13]. (Note that not all states can be described within this framework.) As before, each qubit propagates through its black box. After leaving them, the qubits' state encodes the truth values of the following N independent binary propositions (negating the false propositions, one has N true ones which serve as axioms):

$$(\mathrm{H}_p) \quad \text{“}\textstyle\sum_{j=1}^{N}[n_j(p)\,f_j(0) + m_j(p)\,f_j(1)] = 0.\text{”}$$

with $p = 1, \dots, N$. In suitable measurements quantum mechanics provides a way to test whether certain propositions are decidable or not. If one measures the operator of the Pauli group [12]

$$\hat{\Theta} \equiv \mathrm{i}^{\alpha_1\beta_1}\,\hat{\sigma}_x^{\alpha_1}\,\hat{\sigma}_z^{\beta_1} \otimes \cdots \otimes \mathrm{i}^{\alpha_N\beta_N}\,\hat{\sigma}_x^{\alpha_N}\,\hat{\sigma}_z^{\beta_N}\,, \tag{7}$$

with $\alpha_j, \beta_j \in \{0, 1\}$, one tests whether the proposition

$$(\mathrm{J}) \quad \text{“}\textstyle\sum_{j=1}^{N}[\beta_j\,f_j(0) + \alpha_j\,f_j(1)] = 0.\text{”}$$

is decidable or not. The proposition (J) can be represented as the $2N$-dimensional proposition vector $\vec{J} = (\alpha_1, \dots, \alpha_N, \beta_1, \dots, \beta_N)$ with binary entries. Therefore, there are 4^N different (J)'s. For all decidable propositions the vectors $\vec{J}$ are linear combinations of the vectors $\vec{H}_p = (m_1(p), \dots, m_N(p), n_1(p), \dots, n_N(p))$ representing the axioms, i.e. $\vec{J} = \sum_{p=1}^{N} k_p \vec{H}_p$. Since α_j, β_j are binary, the coefficients must also be binary: $k_p \in \{0, 1\}$. This gives 2^N decidable propositions (J). The corresponding operators $\hat{\Theta}$ can be written as the products $\hat{\Omega}_1^{k_1} \cdots \hat{\Omega}_N^{k_N}$. In this case $\hat{\Theta}$ commutes with all the $\hat{\Omega}_p$'s, and the quantum mechanical formalism implies that the measurement of $\hat{\Theta}$ has a definite outcome. The measurements of all the remaining $4^N - 2^N = 2^N(2^N - 1)$ operators $\hat{\Theta}$ give random outcomes, and the corresponding propositions (J) are undecidable. Note that there are many more undecidable propositions of the form (J) than decidable ones. The ratio between their numbers increases exponentially with the number of qubits, i.e. $\frac{2^N(2^N-1)}{2^N} = O(2^N)$.

In logic one can always complete the axiomatic system by adding new axioms to the set of (H_p) such that any proposition (J) becomes decidable. However, this would require the axioms to be encoded in more than N qubits. Having only N qubits, projecting these qubits into new quantum states, and propagating them through their black boxes, new propositions can become axioms but only if some or all previous axioms become undecidable propositions. This is a consequence of the limited information content of the quantum state.

We have proved that a proposition of the type (J) is (partially) undecidable within the axiomatic system (H_p) if and only if the corresponding measurement $\hat{\Theta}$ from the Pauli group is not commuting with at least one $\hat{\Omega}_p$. Note that one does not need to first prove the mathematical (un)decidability of a proposition by logic before one is able to identify the experiment to test it. For a given set of (H_p), defining an N-bit axiom, one must prepare a joint eigenstate of N commuting tensor products $\hat{\Omega}_p$. In order to test the (un)decidability of a new proposition (J), one needs to measure the operator $\hat{\Theta}$ that corresponds to (J) in this state. The procedures of preparation and measurement can be performed without knowing whether (J) is logically independent from the set of (H_p).

The novelty of multi-bit axioms is the existence of partial undecidability. The two bits of proposition (E) described above correspond to the set of independent commuting operators $\hat{\Omega}_1 = \hat{\sigma}_z \otimes \hat{\sigma}_z$ and $\hat{\Omega}_2 = \hat{\sigma}_x \otimes \hat{\sigma}_x$. The common eigenbasis of these operators is spanned by the maximally entangled Bell states (basis b_{E}): $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1 |z+\rangle_2 \pm |z-\rangle_1 |z-\rangle_2\right)$, $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1 |z-\rangle_2 \pm |z-\rangle_1 |z+\rangle_2\right)$, where e.g. $|z\pm\rangle_1$ denotes the eigenstate with the eigenvalue ± 1 of $\hat{\sigma}_z$ for the first qubit. Thus, after the black boxes the four Bell states encode the four possible truth values of the elementary propositions in (E) and a so-called Bell State Analyzer [14] (i.e. an apparatus that measures in the Bell basis) reveals these values. In the same way, the truth values of the elementary propositions in (F) are encoded in the eigenstates of local $\hat{\sigma}_z$ bases, i.e. by the four states $|z\pm\rangle_1 |z\pm\rangle_2$ (basis b_{F}). Finally, the elementary propositions in (D) are linked with the four product states $|z\pm\rangle_1 |x\pm\rangle_2$ (basis b_{D}). In general, if all the axioms involve joint properties of Boolean functions the multi-partite state encoding these axioms must be entangled.

The Appendix shows the results of a two-photon experiment illustrating how partial and full undecidability are manifested in the randomness of outcomes. We initially prepared a photonic Bell state and encoded properties of two Boolean functions, $f_1(x)$ and $f_2(x)$. First, measurements in the Bell basis, b_{E}, prove that the entangled state indeed encodes joint properties of the two functions, i.e. information about (E). Measurements in other bases can then be interpreted in terms of "partial" and "full" undecidability. Proposition (D) is fully undecidable given (E) as an axiom and the measurement results are completely random. On the other hand, proposition (F) is partially undecidable, disclosed by the fact that two (out of four) outcomes never occur, while the two remaining occur randomly, i.e. each with probability $\frac{1}{2}$. This is illustrated in Figure 4 of the Appendix.

When the outcome of a quantum measurement is definite, it need not possess an *a priori* relation to the actual truth value of a decidable proposition as imposed by classical logic. This can be demonstrated for three qubits initially in the Greenberger-Horne-Zeilinger (GHZ) state [15]

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1 |z+\rangle_2 |z+\rangle_3 + |z-\rangle_1 |z-\rangle_2 |z-\rangle_3\right). \tag{8}$$

We choose as axioms the propositions

$$\begin{array}{ll} (\mathrm{K}_1) & \text{“}f_1(0)+f_1(1)+f_2(0)+f_2(1)+f_3(1)=1.\text{”} \\ (\mathrm{K}_2) & \text{“}f_1(0)+f_1(1)+f_2(1)+f_3(0)+f_3(1)=1.\text{”} \\ (\mathrm{K}_3) & \text{“}f_1(1)+f_2(0)+f_2(1)+f_3(0)+f_3(1)=1.\text{”} \end{array}$$

linked with the operators $\hat{\sigma}_y \otimes \hat{\sigma}_y \otimes \hat{\sigma}_x$, $\hat{\sigma}_y \otimes \hat{\sigma}_x \otimes \hat{\sigma}_y$, and $\hat{\sigma}_x \otimes \hat{\sigma}_y \otimes \hat{\sigma}_y$, respectively. One can *logically* derive from (K_1) to (K_3) the true proposition

$$(\mathrm{L}) \quad \text{“}f_1(1)+f_2(1)+f_3(1)=1.\text{”}$$

On the other hand, the proposition (L) is identified with the measurement of $\hat{\sigma}_x \otimes \hat{\sigma}_x \otimes \hat{\sigma}_x$, but the result imposed by quantum mechanics corresponds to the *negation* of (L), namely: "$f_1(1) + f_2(1) + f_3(1) = 0$." This is the heart of the GHZ argument [15, 16, 17]. In the (standard logical) derivation of (L) the individual function values are well defined and the same, independently of the axiom (K_i) in which they appear. Since this is equivalent to the assumption of non-contextuality [18, 19], the truth values of decidable propositions found in quantum experiments do not necessarily have to be the same as the ones derived by classical logic. Nonetheless, there is a one-to-one correspondence between definiteness (or randomness) of the measurement outcomes and the associated propositions being decidable (or undecidable) within axiomatic set. As shown above, this correspondence is independent of the rules used to infer the specific truth values of the propositions (e.g. classical logic or quantum theory).

One might raise the question whether a classical device can be constructed to reveal the undecidability of propositions. All operations in the experimental test belong to the Clifford group subset of quantum gates and therefore can be efficiently simulated classically [12, 20, 21]. A classical device is possible, provided one uses more resources: N classical bits are required to propagate through the black box in order to specify the N-bit axiomatic set and additional bits are required to model randomness in measurements corresponding to undecidable propositions. (Specifically, $2N$ classical bits propagating through the black box are known to be sufficient to specify definite outcomes in the measurements corresponding to the axioms and random outcomes in the measurements of fully undecidable propositions [22, 23].) Such a device can give the truth values of decidable propositions according to classical logic. On the level of elementary physical systems, however, the world is known to be quantum. It is intriguing that nature supplies us with physical systems that can reveal decidability but cannot be used to learn the classical truth values.

A historic point finally deserves comment. The inference that classical logic cannot capture the structure of quantum mechanics was made by Birkhoff and von Neumann and started the field of quantum logic [24]. Our identification of mathematics/logic with quantum physics is related to, but yet distinct from their approach. Quantum logic was invented to provide an understanding of quantum physics in terms of a set of non-classical logical rules for propositions which are identified with projective quantum measurements. However, "one requires the entire theoretical machinery of quantum mechanics to justify quantum logic" [25]. Our approach aims at providing a justification for quantum randomness starting from purely mathematical propositions and systems with limited information content.

The no-go theorems of Bell [26] and Kochen and Specker [18] prove that quantum randomness cannot be understood as stemming from the ignorance of a hidden variable substructure without coming into conflict with locality and non-contextuality. This suggests that quantum randomness might be of *irreducible* (objective) nature and a consequence of fundamentally limited information content of physical systems, namely N bits in N qubits [4]. If one adopts this view, the present work explains in which experiments the outcomes will be irreducibly random, namely in those that correspond to mathematically undecidable propositions.

After leaving the black boxes the N qubits' quantum states encode exactly N bits of information about Boolean functions, i.e. the systems encode an N-bit *axiom*, and the other logically complementary propositions are undecidable within this axiom. If there exists no underlying (hidden variable) structure, no information is left for specifying their truth values. However, the qubits can be measured in the bases corresponding to undecidable propositions, and – as in any measurement – will inevitably give outcomes, e.g. "clicks" in detectors. These clicks must not contain any information whatsoever about the truth value of the undecidable proposition. Therefore, the individual quantum outcomes must be random, reconciling mathematical undecidability with the fact that a quantum system always gives an "answer" when "asked" in an experiment. This provides an intuitive understanding of quantum randomness, a key quantum feature, using mathematical reasoning. Moreover, the same argument implies that randomness necessarily occurs in any physical theory of systems with limited information content in which measurements are operationally identified with asking questions about undecidable propositions.

In conclusion, we have demonstrated that the decidability or undecidability of certain mathematical propositions in a finite axiomatic set can be tested by performing corresponding Pauli group measurements. This is achieved via an isomorphism between axioms and quantum states as well as between propositions and quantum measurements. Decidability (undecidability) is revealed by definite (random) outcomes. Having this isomorphism, mathematical undecidability needs not to be proved by logics but can be inferred from experimental results. From the foundational point of view, this sheds new light on the (mathematical) origin of quantum randomness in these measurements. Under the assumption that the information content of N elementary physical systems (i.e. qubits) is *fundamentally restricted* to N bits such that no underlying (hidden variable) structure exists, measurement outcomes corresponding to mathematically undecidable propositions must be irreducibly random.

Acknowledgements. We are grateful to G. J. Chaitin for discussions. We acknowledge financial support from the Austrian Science Fund (FWF), the Doctoral Program CoQuS (FWF), the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate, the Marie Curie Research Training Network EMALI, the IARPA-funded U.S. Army Research Office, and the Foundational Questions Institute (FQXi).

Appendix

Here, we describe experiments which were conducted in order to illustrate the concepts developed in the main text. In the case of a single Boolean function $f(x)$, we use the polarization of single photons as information carriers of binary properties encoded by the configuration in the "black box". The single photons are generated in the process of spontaneous parametric down-conversion (SPDC) [10]. The horizontal/vertical linear, $+45°/-45°$ linear, right/left circular polarization of the photon corresponds to eigenstates $|z\pm\rangle$, $|x\pm\rangle$, and $|y\pm\rangle$ of the Pauli operators, respectively. We start by initializing the qubit in a definite polarization state by inserting a linear polarizer in the beam path. The qubit then propagates through the black box in which the Boolean functions are encoded with the help of half-wave plates (HWP) which implement the product of Pauli operators $\hat{\sigma}_x^{f(0)}\,\hat{\sigma}_z^{f(1)}$, eq. (2). Subsequently, measurements of $\hat{\sigma}_z$, $\hat{\sigma}_x$, and $\hat{\sigma}_y$, which test the truth value of a specific proposition, are performed as projective measurements in the corresponding polarization basis. Specifically, to perform $\hat{\sigma}_z$ measurements we use a polarizing beam-splitter (PBS) whose output modes are fiber-coupled to single-photon detector modules and use wave plates in front of the PBS to change the measurement basis. The truth value of the proposition now corresponds to photon detection in one of the two output modes of the PBS.

First, we confirm that complementary quantum measurements indeed reveal truth values of respective logically complementary propositions. To achieve this we prepare the system in a state belonging to the basis in which we

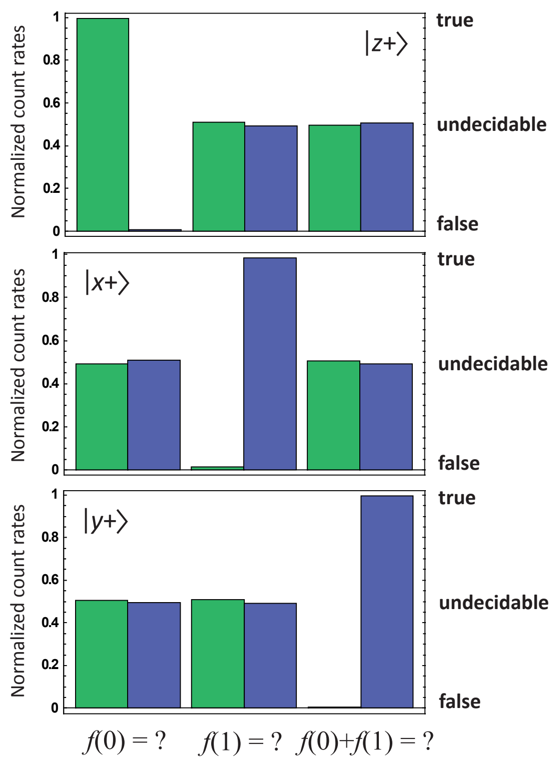

FIG. 3: We input the qubit in a well-defined Pauli operator eigenstate $|z+\rangle$, $|x+\rangle$, or $|y+\rangle$ into the black box, shown from top to bottom. The black box encodes two classical bits, $f(0)$ and $f(1)$, and the measurement is chosen such that the single bit $f(0)$, $f(1)$, or $f(0)+f(1)$, is read out. For every input state we measure in all three complementary bases, i.e., z [asking for $f(0)$], x [$f(1)$], and y [$f(0)+f(1)$], shown from left to right. The three measurements are related to three logically complementary questions (A), (B), (C) of the main text as indicated by the labels. This particular plot is the experimentally obtained data for the black box realizing the function y_1. Similar results were obtained for the other black box configurations y_0, y_2, and y_3. Green (blue) bars represent outcomes "0" ("1") in the respective detectors, giving the answer to the corresponding question. Each input state, after leaving the black box, reveals the truth value of one and only one of the propositions, i.e. it encodes a one-bit axiom. Given this axiom, the remaining two logically complementary propositions are undecidable. This undecidability is revealed by complete randomness of the outcomes in the other two measurement bases. Statistical errors are at most 0.03 % in each graph and therefore not visible.

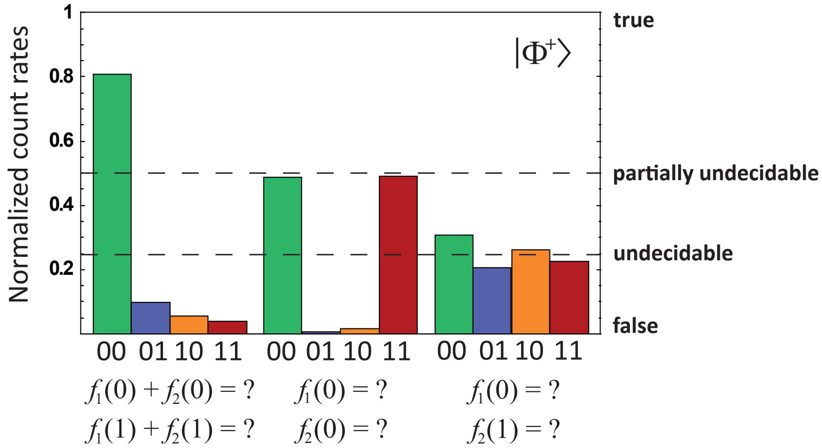

FIG. 4: In this two-qubit experiment a $|\Phi^+\rangle$ Bell state is measured in three different bases (the Bell basis as well as $|z\pm\rangle_1 |z\pm\rangle_2$ and $|z\pm\rangle_1 |x\pm\rangle_2$, shown from left to right). Plotted are the normalized count rates associated with the relevant detector combinations for the black box encoding function y_2 on both photons. The first (second) label gives the answer to the upper (lower) question. The results of the measurements performed in the Bell basis show that the two qubits encode proposition (E) of the main text. The data in the middle plot reveal partial undecidability of proposition (F), given (E) as an axiom, as indicated by the random outcomes in two out of four detector combinations. In contrast, the right plot presents the data corresponding to the fully undecidable proposition (D), where the outcomes are completely random. Similar results for propositions (E), (F) and (D) were obtained for other black box encodings. The reason for the fact that the Bell state in the left plot is not identified with unit fidelity stems from imperfections in the experimental setup (cf. Reference [28]). Unequal detector efficiencies explain the small bias in the right plot. Statistical errors are at most 2 % for the left plot and at most 0.1 % for the other plots and therefore not visible.

finally measure. Specifically, we verify that a measurement in the z basis gives the value of $f(0)$ and similarly, measurements in x and y bases give the value of $f(1)$ and $f(0) + f(1)$, respectively.

Next, we demonstrate that decidable (undecidable) propositions are identified by a sequence of definite (random) outcomes of quantum measurements. For each of the three choices of the initial state, we "ask" all three logically complementary questions by measuring in all three different complementary bases. Figure 3 shows that for every input state one and only one question has a definite answer. This is the axiom encoded in the system leaving black box. The remaining propositions are undecidable given that axiom. This is signified by the observation that the corresponding measurement outcomes are completely random, i.e. evenly distributed.

In the case of two Boolean functions, $f_1(x)$ and $f_2(x)$, we prepare two-photon states with the help of SPDC. The encoding of these functions within the black boxes is done akin to the single-qubit case. We start our investigation by confirming that the truth values of the (elementary) propositions in (E), (F) and (D) are revealed by measurements performed in the bases b_{E}, b_{F} and b_{D} of the main text, respectively. As in the single-qubit case, preparation and measurement are in the same basis (results not shown). Next, we prepare the $|\Phi^+\rangle$ Bell state and measure it in the bases b_{E}, b_{F} and b_{D}. As can be seen in the left plot of Figure 4, measurements in the Bell basis, b_{E}, prove that the entangled state indeed encodes joint properties of the functions $f_1(x)$ and $f_2(x)$, i.e. information about (E). These joint two-qubit measurements require a so-called Bell State Analyzer (BSA) [14, 27, 28], the heart of which is a non-linear gate, such as a controlled-NOT gate [29, 30, 31, 32]. For experimental details see Reference [28]. Measurements in other bases can then be interpreted in terms of "partial" and "full" undecidability. Proposition (D) is fully undecidable given (E) as an axiom encoded as into the photons leaving the black boxes. This can be seen from the right part in Figure 4, in which all four measurement outcomes occur with equal probability. On the other hand, proposition (F) is partially undecidable. This is experimentally revealed by the count distribution of the middle part in Figure 4. The partial undecidability is disclosed by the randomness of the two occurring outcomes, while the other two outcomes do not appear.

* Permanent address: *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore, Singapore*

† Permanent address: *Complex Systems Research Group, HNO, Medical University of Vienna, Währinger Gürtel 18-20, 1090 Wien, Austria*

[1] G. J. Chaitin, Int. J. Theor. Phys. **21**, 941 (1982).
[2] C. S. Calude and H. Jürgensen, Adv. Appl. Math. **35**, 1 (2005).
[3] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[4] A. Zeilinger, Found. Phys. **29**, 631 (1999).
[5] K. Svozil, Phys. Lett. A **143**, 433 (1990).
[6] C. S. Calude and M. A. Stay, Int J. Theor. Phys. **44**, 1053 (2005).
[7] K. Gödel, Monatsheft für Mathematik und Physik (Akademische Verlagsgesellschaft Leipzig) **38**, 173 (1931).
[8] E. Nagel and J. R. Newman, *Gödel's proof* (New York University Press, 1960).
[9] D. Hilbert, *Foundations of Geometry* (Open Court, 1971).
[10] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[11] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[13] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[14] H. Weinfurter, Europhys. Lett. **25**, 559 (1994).
[15] D. Greenberger, M. A. Horne, and A. Zeilinger, in: *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, ed. M. Kafatos (Kluwer Academic Publishers, 1989); electronic version: arXiv:0712.0921v1 [quant-ph].
[16] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[17] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, Nature **403**, 515 (2000).
[18] S. Kochen and E. Specker, Journal of Mathematics and Mechanics **17**, 59 (1967).
[19] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, 1995).
[20] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).
[21] S. Anders and H. J. Briegel, Phys. Rev. A **73**, 022334 (2006).
[22] R. Spekkens, Phys. Rev. A **75**, 032110 (2007).
[23] T. Paterek, B. Dakić, and Č. Brukner, arXiv:0804.2193v1 [quant-ph].
[24] G. Birkhoff and J. von Neumann, Ann. Math. **37**, 823 (1936).
[25] I. Pitowski, *Quantum Probability – Quantum Logic* (Springer, 1989).
[26] J. S. Bell, Physics (N.Y.) **1**, 195 (1964).
[27] M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. A **72**, 1209(R) (1996).
[28] P. Walther and A. Zeilinger, Phys. Rev. A **72**, 010302(R) (2005).
[29] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[30] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. Lett. **88**, 257902 (2002).
[31] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature **426**, 264 (2003).
[32] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, Phys. Rev. Lett. **92**, 020504 (2004).