OPEN ACCESS

Logical independence and quantum randomness

New Journal of Physics
The open-access journal for physics

Logical independence and quantum randomness

T Paterek[1,3,5], J Kofler[1,2], R Prevedel[2], P Klimek[2,4], M Aspelmeyer[1,2], A Zeilinger[1,2] and Č Brukner[1,2]

[1] Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria
[2] Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria
E-mail: tomasz.paterek@univie.ac.at

New Journal of Physics **12** (2010) 013019 (10pp)
Received 14 July 2009
Published 20 January 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/1/013019

Abstract. We propose a link between logical independence and quantum physics. We demonstrate that quantum systems in the eigenstates of Pauli group operators are capable of encoding mathematical axioms and show that Pauli group quantum measurements are capable of revealing whether or not a given proposition is logically dependent on the axiomatic system. Whenever a mathematical proposition is logically independent of the axioms encoded in the measured state, the measurement associated with the proposition gives random outcomes. This allows for an experimental test of logical independence. Conversely, it also allows for an explanation of the probabilities of random outcomes observed in Pauli group measurements from logical independence without invoking quantum theory. The axiomatic systems we study can be completed and are therefore *not* subject to Gödel's incompleteness theorem.

As opposed to the case of classical statistical physics, the theorems by Kochen and Specker [1] and Bell [2] opened up the possibility of viewing probabilities in quantum physics as irreducible and not as stemming from our ignorance about some (non-contextual or local) predeterminated properties. Adopting this view, one can ask if there is any reason why such irreducible probabilities should have different values at all. Here we show that—at least in a certain

[3] Present address: Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542 Singapore, Singapore.
[4] Present address: Complex Systems Research Group, HNO, Medical University of Vienna, Währinger Gürtel 18-20, 1090 Wien, Austria.
[5] Author to whom any correspondence should be addressed.

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

Figure 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 $k = 0, 1, 2, 3$.

subset of measurements (Pauli group measurements)—quantum probabilities can be seen as following from logical independence of mathematical propositions that are associated with the measurements without invoking quantum theory itself.

Any formal system is based on axioms, which are propositions that are defined to be true. Whenever a proposition and a given set of axioms together contain more information than the axioms themselves, the proposition can be neither proved nor disproved from the axioms—it is *logically independent* (or mathematically undecidable [3, 4]). If a proposition is independent of the axioms, neither the proposition itself nor its negation creates an inconsistency together with the axiomatic system.

We demonstrate that the states of 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 [5, 6], thus limiting the information content of the set of axioms. We show that quantum measurements are capable of revealing whether a given proposition is independent or not of the set of axioms. Whenever a mathematical proposition is independent of the axioms encoded in the state, the measurement associated with the proposition gives random outcomes. This allows for an *experimental* test of logical independence by realizing in the laboratory both the actual quantum states and the required quantum measurements. Our axiomatic systems can be completed and are therefore *not* subject to Gödel's incompleteness theorem [7, 8].

Intuitively, independent propositions contain entirely *new information* that cannot be reduced to the information in the axioms. This point of view is related to Chaitin's information-theoretical formulation of logical independence [3, 4]. 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:

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

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 logically independent. Knowing the truth value of one of them does not allow one 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 also know the truth value of (B). Hence, proposition (B) is logically independent from the system containing the single axiom (A). Another example of an independent proposition within the same axiomatic system is:

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

Again, this statement can be neither proved nor disproved from 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)–(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 value for argument "0", i.e. $f_1(0) = f_2(0)$.'
'The functions have the same value 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. 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 elementary propositions in (D).

A qualitatively new aspect of multi-bit axioms is the existence of 'partially' independent propositions, i.e. propositions that contain more than one elementary proposition, of which only some are independent. An example of such a partially independent 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 of deciding the second elementary proposition leads to partial independence of proposition (F). In a similar way, proposition (F) is partially independent of 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 independence 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 $\hat{\sigma}_y = i\hat{\sigma}_x\,\hat{\sigma}_z$, 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

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

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

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

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 proposition (A). This one bit is the maximal amount of information that can be encoded in a qubit [5, 6].

Mathematics/logic		Quantum physics
Axioms of limited information content	↔	Quantum states
Boolean functions	↔	Unitary transformations
Question about proposition	↔	Quantum measurement
Logical dependence/independence	↔	Definiteness/randomness of outcomes

Figure 2. Link between logical independence and quantum randomness.

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 *independent* from 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 independent of the one-bit axiom (A). This links logical independence and quantum randomness in complementary measurements. We propose that it is therefore possible to *experimentally* find out whether a proposition is logically independent 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 dependent or independent proposition. Therefore, any quantum experiment revealing logical independence requires many repetitions. (It can be shown that—given a certain level of noise—the probability to infer wrongly whether the proposition is dependent or not decays exponentially with the length of the outcome string.)

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

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

with $m_j(p), n_j(p) \in \{0, 1\}$. A broad family of such states is the family of stabilizer [10, 11] and graph states [12]. (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):

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

In suitable measurements quantum mechanics provides a way of testing whether certain propositions are dependent or not. If one measures the operator of the Pauli group [11]

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

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

$$\text{(J)} \quad \text{`}\sum_{j=1}^{N}[\beta_j\, f_j(0) + \alpha_j\, f_j(1)] = 0\text{'}$$

is dependent or not. The proposition (J) can be represented as the $2N$-dimensional proposition vector $\vec{J} = (\alpha_1, \ldots, \alpha_N, \beta_1, \ldots, \beta_N)$ with binary entries. Therefore, there are 4^N different (J)s. For all dependent propositions, the vectors $\vec{J}$ are linear combinations of the vectors $\vec{H}_p = (m_1(p), \ldots, m_N(p), n_1(p), \ldots, n_N(p))$ 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 dependent 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 independent. Note that there are many more independent propositions of the form (J) than dependent 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 dependent. 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 independent propositions. This is a consequence of the limited information content of the quantum system.

We have proved that a proposition of type (J) is dependent on the axiomatic system (H_p) if and only if the corresponding measurement $\hat{\Theta}$ from the Pauli group is commuting with all $\hat{\Omega}_p$. Note that one does not need to first prove the (in)dependence 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 operators $\hat{\Omega}_p$. In order to test the logical (in)dependence 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 of the set of (H_p).

The measurement $\hat{\Theta}$ is highly degenerate because it tests the logical (in)dependence of the binary proposition (J) of the axioms. Less degenerate measurements are possible, which simultaneously test the logical (in)dependence of several elementary propositions of the form (J). Such multi-bit propositions contain many elementary propositions. If not all of them are independent of the axioms, this gives rise to partial independence. This provides an explanation for different values of outcome probabilities in Pauli group measurements, which is based on logic without invoking quantum theory. A measurement corresponding to any single independent elementary proposition (with two possible measurement outcomes) gives uniformly random results. In a measurement whose outcomes reveal the independence

of m independent elementary propositions (with 2^m possible measurement outcomes), these outcomes occur with probabilities $\frac{1}{2^m}$. (The results revealing dependence of elementary propositions are always definite.)

To illustrate the idea of multi-bit propositions and partial independence, consider proposition (E) described above. Its elementary propositions 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}): $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|z+\rangle_1|z+\rangle_2 \pm |z-\rangle_1|z-\rangle_2)$, $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|z+\rangle_1|z-\rangle_2 \pm |z-\rangle_1|z+\rangle_2)$, 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 [13] (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.

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' independence. Proposition (D) is fully independent given (E) as an axiom, and the four possible measurement results are completely random with probabilities of $\frac{1}{4}$. On the other hand, proposition (F) is partially independent, which is disclosed by the fact that two (out of four) outcomes never occur, while the two remaining occur randomly, i.e. each with probability $\frac{1}{2}$.

When the outcome of a quantum measurement is definite, it need not possess an *a priori* relation to the actual truth value of a dependent proposition as imposed by classical logic. This can be demonstrated for three qubits initially in the Greenberger–Horne–Zeilinger (GHZ) state [14]:

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

We choose as axioms the propositions

$$(\mathrm{K}_1) \quad `f_1(0) + f_1(1) + f_2(0) + f_2(1) + f_3(1) = 1.'$$
$$(\mathrm{K}_2) \quad `f_1(0) + f_1(1) + f_2(1) + f_3(0) + f_3(1) = 1.'$$
$$(\mathrm{K}_3) \quad `f_1(1) + f_2(0) + f_2(1) + f_3(0) + f_3(1) = 1.'$$

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

$$(\mathrm{L}) \quad `f_1(1) + f_2(1) + f_3(1) = 1.'$$

On the other hand, 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 [14]–[16]. In the (standard logical) derivation of (L), the individual function values are well defined and are the *same*,

independently of the axiom (K_i) in which they appear. Since this is equivalent to the assumption of non-contextuality [1, 17], the truth values of dependent 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 dependent (or independent) within the 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 as to whether a classical device can be constructed to reveal the independence of propositions. All operations in the experimental test belong to the Clifford group subset of quantum gates and therefore can be efficiently simulated classically [11, 18, 19]. A classical device is possible, given sufficient 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 independent 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 independent propositions [20, 21].) Such a device can give the truth values of dependent 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 logical dependence but cannot be used to learn the classical truth values.

Finally, a historic point deserves comment. The inference that classical logic cannot capture the structure of quantum mechanics was made by Birkhoff and von Neumann [22] and started the field of quantum logic. Our link between mathematics/logic and certain elements of 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 that are identified with projective quantum measurements. However, 'one requires the entire theoretical machinery of quantum mechanics to justify quantum logic' [23]. Our approach aims at providing a justification for quantum randomness starting from an operational representation of purely mathematical propositions and systems with limited information content.

The no-go theorems of Bell [2] and Kochen and Specker [1] prove that quantum randomness cannot be understood as stemming from the ignorance of a hidden variable substructure without coming into conflict with local realism and non-contextuality. This suggests that quantum randomness might be of *irreducible* (objective) nature [24, 25] and a consequence of fundamentally limited information content of physical systems, namely N bits in N qubits [6]. If one adopts this view, the present work explains which experiments will have irreducibly random outcomes, namely those that correspond to logically independent 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 independent of 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 independent 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 independent

proposition. Therefore, the individual quantum outcomes must be random, reconciling logical independence 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 independent propositions [26].

In conclusion, we have demonstrated that the dependence or independence of certain mathematical propositions in a finite axiomatic set can be tested by performing corresponding Pauli group measurements. (It would be interesting to investigate the possiblity of extending our results beyond this class of measurements.) This is achieved via an isomorphism between axioms and quantum states as well as between propositions and quantum measurements. Dependence (independence) is revealed by definite (random) outcomes. Having this isomorphism, logical independence need not be proved by logic 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 logically independent propositions must be irreducibly random.

The results of a recent experimental demonstration of the concepts introduced in this paper can be found in the e-print [27].

Acknowledgments

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 US Army Research Office and the Foundational Questions Institute (FQXi).

References

[1] Kochen S and Specker E 1967 *J. Math. Mech.* **17** 59
[2] Bell J S 1964 *Physics* **1** 195
[3] Chaitin G J 1982 *Int. J. Theor. Phys.* **21** 941
[4] Calude C S and Jürgensen H 2005 *Adv. Appl. Math.* **35** 1
[5] Holevo A S 1973 *Probl. Inf. Transm.* **9** 177
[6] Zeilinger A 1999 *Found. Phys.* **29** 631
[7] Gödel K 1931 *Monhefte Math. Phys.* **38** 173
[8] Nagel E and Newman J R 1960 *Gödel's Proof* (New York: New York University Press)
[9] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 *Phys. Rev. Lett.* **75** 4337
[10] Gottesman D 1996 *Phys. Rev.* A **54** 1862
[11] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[12] Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev.* A **68** 022312
[13] Weinfurter H 1994 *Europhys. Lett.* **25** 559

[14] Greenberger D, Horne M A and Zeilinger A 1989 in: *Bell's Theorem, Quantum Theory, and Conceptions of the Universe,* ed M Kafatos (Dordrecht: Kluwer)
[15] Mermin N D 1990 *Phys. Rev. Lett.* **65** 1838
[16] Pan J-W, Bouwmeester D, Daniell M, Weinfurter H and Zeilinger A 2000 *Nature* **403** 515
[17] Peres A 1995 *Quantum Theory: Concepts and Methods* (Dordrecht: Kluwer)
[18] Aaronson S and Gottesman D 2004 *Phys. Rev.* A **70** 052328
[19] Anders S and Briegel H J 2006 *Phys. Rev.* A **73** 022334
[20] Spekkens R 2007 *Phys. Rev.* A **75** 032110
[21] Paterek T, Dakić B and Brukner Č 2009 *Phys. Rev.* A **79** 012109
[22] Birkhoff G and von Neumann J 1936 *Ann. Math.* **37** 823
[23] Pitowski I 1989 *Quantum Probability—Quantum Logic* (Berlin: Springer)
[24] Svozil K 1990 *Phys. Lett.* A **143** 433
[25] Calude C S and Stay M A 2005 *Int. J. Theor. Phys.* **44** 1053
[26] Paterek T, Dakić B and Brukner Č 2008 arXiv:0804.1423
[27] Paterek T, Kofler J, Prevedel R, Klimek P, Aspelmeyer M, Zeilinger A and Brukner Č 2008 arXiv:0811.4542