

# Quantum complementarity and logical indeterminacy

Časlav Brukner

Published online: 19 February 2009  
© Springer Science+Business Media B.V. 2009

**Abstract** Whenever a mathematical proposition to be proved requires more information than it is contained in an axiomatic system, it can neither be proved nor disproved, i.e. it is undecidable, or logically undetermined, within this axiomatic system. I will show that certain mathematical propositions on a  $d$ -valent function of a binary argument can be encoded in  $d$ -dimensional quantum states of mutually unbiased basis (MUB) sets, and truth values of the propositions can be tested in MUB measurements. I will then show that a proposition is undecidable within the system of axioms encoded in the state, if and only if the measurement associated with the proposition gives completely random outcomes.

**Keywords** Quantum complementarity · Logical indeterminacy · Mathematical undecidability

The theorems of Bell (1964), Kochen and Specker (1967) as well as of Greenberger et al. (1989) showed that the mere concept of co-existence of local elements of physical reality is in a contradiction with quantum mechanical predictions. Apart from the known loopholes, which are considered by the majority of physicists to be of technical nature, all experiments confirmed the quantum predictions. This implies that either the assumption of “elements of reality”, or “locality” or both must fail. Most working scientists seem to hold fast to the concept of “elements of reality.” One of the reasons for this tendency might be that it is not clear how to base a theory without this concept. While one should leave all options open, it should be noted that maintaining the assumption of realism and denying locality faces certain conceptual problems (Peres 1995). But, perhaps more importantly in

---

Č. Brukner (✉)

Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences,  
Boltzmanngasse 3, 1090 Vienna, Austria  
e-mail: caslav.brukner@univie.ac.at

Č. Brukner

Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

my view is that so far this approach could not encourage any new phenomenology that might result in the hope for a progressive research program.

An alternative to this is to arrive at a new understanding of probabilities which is not based on our ignorance about some predetermined properties. What is then the origin of probabilities? What makes the probabilities different at all? Here I will show that certain mathematical propositions on a  $d$ -valent function of a binary argument can be encoded in  $d$ -dimensional quantum states (qudits), and truth values of the propositions can be tested in corresponding quantum measurements. I will then show that logically independent propositions correspond to measurements in mutually unbiased basis (MUB) sets. In quantum theory, a pair of orthonormal bases  $\{|k\rangle\}, 0 \leq k \leq d-1$  and  $\{|l\rangle\}, 0 \leq l \leq d-1$  in a Hilbert space  $\mathbb{C}^d$  are said to be unbiased if the modulus square of the inner product between any basis vector from  $\{|k\rangle\}$  with any other basis vector from  $\{|l\rangle\}$  satisfies  $|\langle k|l\rangle|^2 = 1/d$ . A set of bases for which each pair of bases are unbiased is said to be mutually unbiased (Ivanovic 1981; Wootters and Fields 1989). If one assumes that there is a fundamental limit on how much information a quantum system can carry (“a single qudit carries one dit of information”), and that this information is exhausted in defining one of the propositions (taken as an axiom), then the measurements that correspond to logically independent propositions must give irreducibly random outcomes. This allows to derive the probabilities ( $= 1/d$ ) for outcomes of the MUB measurements without directly invoking quantum theory, but by looking if the proposition is definite or “undecidable” within the axiomatic set.

In 1982, Chaitin gave an information theoretical formulation of mathematical undecidability suggesting that it arises whenever a proposition to be proven and the axioms contain together more information than the set of axioms alone (Chaitin 1982; Calude and Jürgensen 2005). In this work, when relating mathematical undecidability to quantum randomness, I will exclusively refer to the incompleteness in Chaitin’s sense and not to the original work of Gödel. Furthermore, I will consider mathematical undecidability in those axiomatic systems which can be completed and which therefore are *not* subject to Gödel’s incompleteness theorem.<sup>1</sup>

Consider a  $d$ -valent function  $f(x) \in 0, \dots, d-1$  of a single binary argument  $x \in \{0, 1\}$ , with  $d$  a prime number.<sup>2</sup> There are  $d^2$  such functions. We will partition the functions into  $d+1$  different ways following the procedure of Ref. Paterek et al. (2009). In a given partition, the  $d^2$  functions will be divided into  $d$  different groups each containing  $d$  functions. Enumerating the first  $d$  partitions by the integer  $a = 0, \dots, d-1$  and the groups by  $b = 0, \dots, d-1$ , the groups of functions are generated from the formula:

$$f(1) = af(0) \oplus b, \quad (1)$$

where the sum is modulo  $d$ . In the last partition, enumerated by  $a = d$ , the functions are divided into groups  $b = 0, \dots, d-1$  according to the functional value  $f(0) = b$ . The functions can be represented in a table in which  $a$  enumerates the rows of the table, while  $b$  enumerates different columns. For all but the last row the table is built in the following way : (i) choose the

<sup>1</sup> For a possible relation between Gödel’s theorem and physics see Barrow (2006). For a relation between algorithmic randomness and quantum indeterminacy see Svozil (1990), Stay and Calude (2005) and Calude and Svozil (2006).

<sup>2</sup> The considerations here can be generalized to all dimensions that are powers of primes. This is related to the fact that in quantum theory in these cases a complete set of mutually unbiased bases is known to exist. In all other cases this is an open question and goes beyond the scope of this paper (see, for example Paterek et al. (2009)).

row,  $a$ , and the column,  $b$ ; (ii) vary  $f(0) = 0, \dots, d-1$  and compute  $f(1)$  according to Eq. (1); (iii) write pairs  $f(0)f(1)$  in the cell. The last row ( $a = d$ ) is built as follows: (i) choose the column  $b$ ; (ii) vary  $f(1) = 0, \dots, d-1$  and put  $f(0) = b$ ; (iii) write pairs  $f(0)f(1)$  in the cell. For example, for  $d = 3$ , one has

| $b = 0$  | $b = 1$  | $b = 2$  |                           |
|----------|----------|----------|---------------------------|
| 00 10 20 | 01 11 21 | 02 12 22 | $"f(1) = b"$              |
| 00 11 22 | 01 12 20 | 02 10 21 | $"f(1) = f(0) \oplus b"$  |
| 00 12 21 | 01 10 22 | 02 11 20 | $"f(1) = 2f(0) \oplus b"$ |
| 00 01 02 | 10 11 12 | 20 21 22 | $"f(0) = b"$              |

All groups (cells in the table) of functions that do not belong to the last row are specified by the proposition:

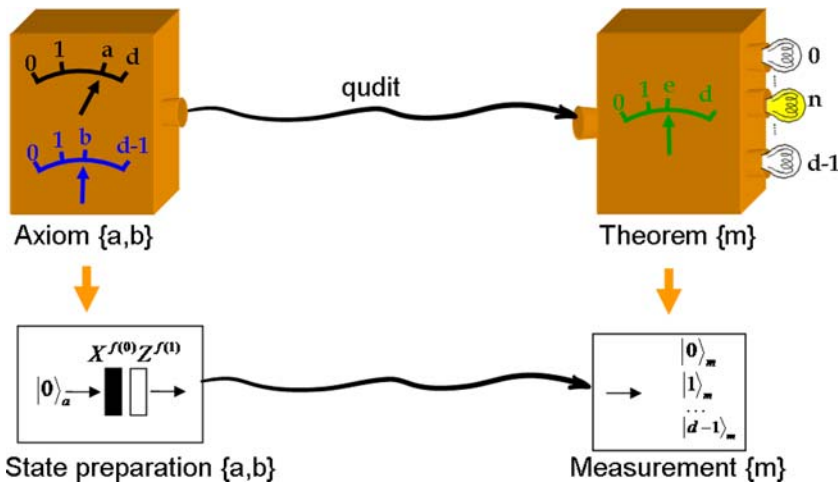
$$\{a, b\} : \text{"The function values } f(0) \text{ and } f(1) \text{ satisfy } f(1) = af(0) \oplus b", \quad (3)$$

while those from the last row ( $a = d$ ) by

$$\{d, b\} : \text{"The function value } f(0) = b". \quad (4)$$

The propositions corresponding to different partitions  $a$  are *independent* from each other. For example, if one postulates the proposition (A) " $f(1) = af(0) \oplus b$ " to be true, i.e. if we choose it as an "axiom", then it is possible to prove that "theorem" (T1) " $f(1) = af(0) \oplus b'$ " is false for all  $b' \neq b$ . Proposition (T1) is decidable within the axiom (A). Within the same axiom (A) it is, however, impossible to prove or disprove "theorem" (T2) " $f(1) = mf(0) \oplus n$  with  $m \neq a$ . Having only axiom (A), i.e. only *one* dit of information, there is not enough information to know also the truth value of (T2). Ascribing truth values to two propositions belonging to two different partitions, e.g. to both (A) and (T2), would require *two* dits of information. Hence, in Chaitin's sense, proposition (T2) is mathematically *undecidable* within the system containing the single axiom (A).

So far, we have made only logical statements. To make a bridge to physics consider a hypothetical device—"preparation device"—that can encode a mathematical axiom  $\{a, b\}$  of the type (3) or (4) into a property of a physical system by setting a "control switch" of the apparatus in a certain position  $\{a, b\}$ . In an operational sense the choice of the mathematical axiom is entirely defined by the switch position as illustrated in Fig. 1 (top). We make no particular assumptions on the physical theory (e.g., classical or quantum) that underlies the behavior of the system, besides that it *fundamentally limits the information content of the system to one dit of information*. Furthermore, we assume that there is a second device—a "measurement apparatus"—that can test the truth value of a chosen mathematical proposition again by setting a control switch of the apparatus to a certain position associated to the proposition. The choice of the switch position  $\{m\}$ ,  $m \in \{0, \dots, d\}$ , corresponds to a performance of one of the  $d + 1$  possible measurements on the system and the occurrence of a  $d$ -valued outcome  $n$  in the measurement is identified with finding proposition  $\{m, n\}$  (of the type (3) or (4)) being true. Consider now a situation where the preparation device is set on  $\{a, b\}$ , while the measurement apparatus on  $\{m\}$ . If  $m = a$ , the outcome confirms the axiom, i.e. one has  $n = b$ . This is why we say that measurement  $\{m\}$  tests mathematical proposition  $\{a, b\}$ . What will be the outcome in a single run of the experiment if  $m \neq a$ ?



**Fig. 1** Quantum experiment testing (un)decidability of mathematical propositions (3) and (4). A qudit ( $d$ -dimensional quantum state) is initialized in a definite quantum state  $|0\rangle_a$  of one of  $d + 1$  mutually unbiased bases sets  $a \in \{0, \dots, d\}$ . Subsequently, the unitary transformation  $\hat{U} = \hat{X}^{f(0)}\hat{Z}^{f(1)}$  which encodes the  $d$ -valued function with functional values  $f(0)$  and  $f(1)$  is applied to the qudit. The final state encodes the proposition: “ $f(1) = af(0) \oplus b$ ” for  $a = 0, \dots, d-1$  or the proposition: “ $f(0) = b$ ” for  $a = d$ . The measurement apparatus is set to measure in the  $m$ -th basis  $\{|0\rangle_m, \dots, |d-1\rangle_m\}$ , which belongs to one of  $d + 1$  mutually unbiased basis sets  $m \in \{0, \dots, d\}$ . It tests the propositions: “ $f(1) = mf(0) \oplus n$ ” for  $m = 0, \dots, d-1$  or “ $f(0) = n$ ” for  $m = d$

I will show that devices from the previous paragraph are not hypothetical at all. In fact, they can be realized in quantum mechanics. The argument is entirely based on Ref. Paterek et al. (2009). In the basis of generalized Pauli operator  $\hat{Z}$ , denoted as  $|\kappa\rangle$ ,  $\kappa \in \{0, \dots, d-1\}$ , we define two elementary operators

$$\hat{Z}|\kappa\rangle = \eta_d^\kappa|\kappa\rangle, \quad \hat{X}|\kappa\rangle = |\kappa + 1\rangle, \quad (5)$$

where  $\eta_d = \exp(i2\pi/d)$  is a complex  $d$ th root of unity. The eigenstates of the  $\hat{X}\hat{Z}^a$  operator,  $a \in \{0, \dots, d-1\}$ , expressed in the  $\hat{Z}$  basis, are given by  $|j\rangle_a = (1/\sqrt{d}) \sum_{\kappa=0}^{d-1} \eta_d^{-j\kappa - as_\kappa} |\kappa\rangle$ , where  $s_\kappa = \kappa + \dots + (d-1)$ , and the  $\hat{Z}$  operator shifts them:  $\hat{Z}|j\rangle_a = |j-1\rangle_a$ . To encode the axiom  $\{a, b\}$  into a quantum state the preparation device is set to prepare state  $|0\rangle_a$  and then to apply the unitary  $\hat{U} = \hat{X}^{f(0)}\hat{Z}^{f(1)}$  on it (Fig. 1, down). The action of the device is, for  $a = 0, \dots, d-1$  and up to a global phase,  $\hat{U} \propto (\hat{X}\hat{Z}^a)^{f(0)}\hat{Z}^b$ , which follows from Eq. (1) and the commutation relation for the elementary operators,  $\hat{Z}\hat{X} = \eta_d\hat{X}\hat{Z}$ . The state leaving the preparation device is shifted exactly  $b$  times resulting in  $|-b\rangle_a$ . For the case  $a = d$  the state is prepared in the eigenstate  $|0\rangle_d \equiv |0\rangle$  of the operator  $\hat{Z}$  and the unitary transforms it into, up to the phase factor,  $|+b\rangle_d$ . When the switch of the measurement apparatus is set to  $\{m\}$  it measures the incoming state in the basis  $\{|0\rangle_m, \dots, |d-1\rangle_m\}$ . For  $m = a$  the measurement will confirm the axiom  $\{a, b\}$  giving outcome  $b$ . In all other cases, the result will be completely random. This follows from the fact that the eigenbases of  $\hat{X}\hat{Z}^a$  for  $a = 0, \dots, d-1$  ( $\hat{Z}^0 \equiv 1$ ) and eigenbasis of  $\hat{Z}$  are known to form a complete set of  $d + 1$  mutually unbiased basis sets (Bandyopadhyay et al. 2002). They have the property that a system prepared in a state from one of the bases will give completely random results if measured in any other basis, i.e.  $|\langle a|b\rangle_n|^2 = 1/d$  for all  $b, n$  and  $a \neq m$ . The previous discussion suggests, however, that probabilities for MUB

measurements can be justified without directly invoking quantum theory, by looking if the proposition is definite, or undecidable, within the axiomatic system. For the analysis of logical propositions and MUB measurements on composite separable and entangled quantum systems see Ref. Paterek et al. (2008).

Most working scientists hold fast to the viewpoint according to which randomness can only arise due to the observer's ignorance about pre-existing properties of physical systems. But the theorems of Kochen and Specker (1967) and Bell (1964) have seriously put such a belief in question. I argue that an alternative viewpoint according to which quantum randomness is irreducible is vindicable. As proposed by Zeilinger (1999) an individual quantum system contains only a limited information content ("a single qudit carries one dit of information"). I have shown here that one can encode a finite set of axioms in a quantum state and test the truth values of mathematical propositions in quantum measurements. If the proposition is decidable within the axiomatic system, the outcome of the measurement will be definite. However, if it is undecidable, the response of the system must not contain any information whatsoever about the truth value of the undecidable proposition, and it cannot "refuse" to give an answer.<sup>3</sup> Unexplained and perhaps unexplainable, it inevitably gives an outcome—a "click" in a detector or a flash of a lamp—whenever measured. I suggest that the individual outcome must then be irreducible random, reconciling mathematical undecidability with the fact that a system always gives an "answer" when "asked" in an experiment.

I am grateful to T. Paterek, R. Prevedel, J. Kofler, P. Klimek, M. Aspelmeyer and A. Zeilinger for numerous discussions on the topic. I acknowledge financial support from the Austrian Science Fund (FWF), the Doctoral Program CoQuS and the European Commission under the Integrated Project Qubit Applications (QAP).

## References

- Bandyopadhyay S, Boykin PO, Roychowdhury V, Vatan F (2002) A new proof for the existence of mutually unbiased bases. *Algorithmica* 34:512
- Barrow JD (2006) Gödel and physics, electronic version: arXiv:physics/0612253. Paper presented at "Horizons of Truth", Kurt Gödel Centenary Meeting, Vienna, 27–29th April 2006
- Bell J (1964) On the Einstein Podolsky Rosen paradox. *Physics* 1:195–200
- Calude CS, Jürgensen H (2005) Is complexity a source of incompleteness? *Appl Math* 35:1–15
- Calude CS, Svozil K (2006) Quantum randomness and value indefiniteness, electronic version: arXiv:quant-ph/0611029
- Chaitin GJ (1982) Gödel's theorem and information. *Int J Theor Phys* 21:941–954
- Greenberger D, Horne MA, Zeilinger A (1989) Going beyond Bell's theorem. In: Kafatos M (ed) *Bell's theorem, quantum theory, and conceptions of the Universe*. Kluwer Academic Publishers, Dordrecht (electronic version: arXiv:0712.0921v1 [quant-ph])
- Ivanovic ID (1981) Geometrical description of quantal state determination. *J Phys A* 14:3241–3245
- Kochen S, Specker E (1967) The problem of hidden variables in quantum mechanics. *J Math Mech* 17:59–87
- Paterek T, Kofler J, Prevedel R, Klimek P, Aspelmeyer M, Zeilinger A, Brukner Č (2008) Mathematical undecidability and quantum randomness, electronic version: arXiv:0811.4542
- Paterek T, Dakić B, Brukner Č (2009) Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models. *Phys Rev A* 79:012109
- Peres A (1995) *Quantum theory: concepts and methods*. Kluwer Academic, Dordrecht, pp 153–154
- Stay MA, Calude CS (2005) From Heisenberg to Gödel via Chaitin. *Int J Theor Phys* 44:1053–1065
- Svozil K (1990) The quantum coin toss-testing microphysical undecidability. *Phys Lett A* 143:433–437
- Wootters WK and Fields BD (1989) Optimal state-determination by mutually unbiased measurements. *Ann Phys (NY)* 191:363–381
- Zeilinger A (1999) A foundational principle for quantum mechanics. *Found Phys* 29:631–643

<sup>3</sup> To put it in a grotesque way the system is not allowed to response "I am undecidable, I cannot give an answer."