4 SUMMIT VIENNA 2015 IS IS

Extended Abstract

Quantum Information with Meaning Inside and Outside the Quantum

Alastair A. Abbott [1,2,*], Cristian S. Calude [1] and Karl Svozil [3,1]

[1] Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand
[2] Centre Cavaillès, École Normale Supérieure, 29 rue d'Ulm, 75005 Paris, France
[3] Institute for Theoretical Physics, Vienna University of Technology, Wiedner Haupstrasse 8-10/136, 1040 Vienna, Austra

E-Mails: a.abbott@auckland.ac.nz (A. A.); cristian@cs.auckland.ac.nz (C. C.); svozil@tuwien.ac.at (K. S.)

* Author to whom correspondence should be addressed;

Accepted: 21 March, 2015

The ability to transfer information securely is essential in the modern world we live in. While the field of cryptography has long researched ways to do this, events over the last couple of years have brought the issues of secure information transfer squarely into the public eye. As a consequence, security and cryptography have quickly become issues of social and political importance, sparking debates about the values of privacy and the role of government.

An essential ingredient of modern cryptography is the generation of randomness: cryptographic techniques are built on the premise that one has access to random bits. It is well known, however, that computers cannot produce algorithmically random sequences – that is, sequences with maximal algorithmic information content – but are doomed to produce 'pseudorandomness'. This lack of randomness can be, and has been, exploited to compromise security, see [4].

The active field of quantum information theory has proposed approaches to provide supposedly 'unbreakable' security by exploiting various quantum phenomena. This security unfortunately relies on assumptions about the nature of quantum measurements and their ability to generate random bits. Anton Zeilinger summarises this by postulating that the simplest quantum systems, qubit, can hold only one bit of classical information [6]. This foundational principle is in line with a wider paradigm shift to view quantum information as an extension of classical information, but it is nonetheless unsatisfying to simply

postulate this principle, given its importance in determining the practical advantages of quantum information theory.

In order to understand better how quantum mechanics can help generate meaningful information, we instead look to relate the outcomes of quantum measurements to formal properties of the system based on more fundamental assumptions.

Indeed, we have shown that a) some of the postulated properties of quantum information follow from the formal structure of the theory and b) a purely formal notion of information within a quantum world can generate, via measurement, meaningful and useful information in the macroscopic world (for example, in cryptography).

The indeterminism of quantum measurements can be formalised via the notion of *value indefiniteness*. To explain this concept, let us consider an arbitrary quantum system and ask whether the outcome of a measurement of any observable quantity A (such as the energy of the system, its angular momentum (spin), etc.) is determined prior to the measurement. If this is the case, then we say the observable is *value definite* with value $v(A)$; otherwise, the observable is *value indefinite* and $v(A)$ is undefined.

Mathematically, one can reduce all observable quantities to so-called projection observables, which can only take the values 0 or 1. Thus, the question of whether the outcome of several measurements can be simultaneously determined in advance can be rephrased in terms of the information 'carried' by a particular system in a definite quantum state. Classically, one expects that all quantities are determined in advance, and hence all observables are value definite. Quantum mechanically, however, the belief is that this is not the case, and the information content of quantum systems is limited.

Formulating carefully the notion of value indefiniteness allows us to formalise the notion of (quantum) indeterminism; however, this doesn't help clarify whether quantum systems are indeed value indefinite or not. Staying in this formal framework, the Kochen-Specker theorem [5] provides a first positive result, showing that at least some observables must be value indefinite if one makes the assumption known as *non-contextuality*, which states that any definite values that exist must be independent of other compatible measurements that may or may not be performed on the system. Under the same assumption, this theorem can be strengthened to show that only one single observable can have the definite value 1 (see [2]). Furthermore, only observables that can be measured simultaneously with this single one can have the definite value 0; the rest must all be value indefinite. Since the preparation of a system involves precisely ensuring that, usually via measurement, the system is in a definite state with respect to some desired observable, this result shows that no other incompatible observable can be value definite. That is, preparing a system in a definite state by making the 'preparation' observable value definite specifies completely the information content of the quantum system. *This is an example of syntactical quantum information acquiring meaning at the level of the quantum itself.*

Can the syntactical information at the level of the quantum generate meaning outside the quantum, that is, at the macroscopic level?

The results cited above hold in the Hilbert-space framework of quantum mechanics and are formulated only in terms of a syntactical notion of information. Their real importance becomes evident when one interprets them in the context of quantum measurements. Specifically, if we prepare a quantum system in a known state, they allow us to 'locate' observables which we can measure, but which are value indefinite; that is, observables whose measurement results are not specified by any pre-existing property of the quantum system. Furthermore, with respect to a mathematical model of unpredictability

which we developed in [3], the results of these measurements can be shown to be *absolutely unpredictable.*

In this way we get a mathematical explanation and justification of the largely accepted intuition that quantum mechanics is inherently unpredictable, and that this unpredictability arises from the phenomenon of indefiniteness within the quantum world.

Furthermore, if one considers a hypothetical infinite sequence generated by the repeated measurement of a quantum value indefinite observable, one can prove that these sequences must be strongly incomputable, technically 'bi-immune' [1]. Such sequences cannot be generated by any Turing machine or classical computer, showing that value indefiniteness leads to a clear classical/quantum split in a purely algorithmic context. Importantly, bi-immunity is a property of observed, macroscopic quantities, quite separate from the quantum framework in which the value indefiniteness is formalised.

This form of macroscopic meaning created from the lack of syntactic information is precisely the scenario that quantum random number generators try to create, and which is essential for the development and certification of quantum cryptographic systems. The fact that the macroscopic information created goes beyond anything classically obtainable serves as a valuable practical resource, outside of and removed from the quantum formalism.

To conclude, *quantum information creates meaning within the quantum and via measure- ment, the lack of information within the quantum, creates meaning and valuable information at the macroscopic level.*

Acknowledgments

The second author thanks Prof. S. Marcus for useful conversations on quantum information theory. This work was supported in part by Marie Curie FP7-PEOPLE-2010-IRSES Grant RANPHYS.

References and Notes

1. Abbott, A.A.; Calude, C.S.; Svozil, K. Strong Kochen-Specker theorem and incomputability of quantum randomness. *Physical Review A* **2012**, *86*, 062109.
2. Abbott, A.A.; Calude, C.S.; Svozil, K. Value-indefinite observables are almost everywhere. *Physical Review A* **2013**, *89*, 032109.
3. Abbott, A.A.; Calude, C.S.; Svozil, K. On the unpredictability of individual quantum measurement outcomes. *CDMTCS Research Report* **2014**, *458*.
4. Calude, C.S. Quantum randomness & cryptology. *CyberTalk* **2013**, *3*, 42–43.
5. Kochen, S.; Specker, E. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* **1967**, *17*, 59–87.
6. Zeilinger, A. A foundational principle for quantum mechanics. *Foundations of Physics* **1999**, *29(4)*,631–643.

© 2015 by the authors; licensee MDPI and ISIS. This abstract is distributed under the terms and conditions of the Creative Commons Attribution license.