Logical loophole in random 3-bit sequence generator

Alexandre de Castro

Laboratório de Matemática Computacional, Centro Nacional de Pesquisa Tecnológica em Informática para a Agricultura (Embrapa Informática Agropecuária), Empresa Brasileira de Pesquisa Agropecuária, Campinas-SP 13083-886, Brazil.

Abstract

In this note, we will provide an information-theoretic framework for the random 3-bit sequence $\{111, 110, 101, 100, 011, 010, 001, 000\}$ that demonstrates (by using Wigner's inequality) a logical loophole in the Bell-CHSH inequality [1, 2, 3], as also has recently been found experimentally for triples measurements [4]. As a consequence of this, both classical and quantum regimes can share their bounds within the same environment, which shows that maximally entangled states used in cryptography secure systems can be critically subverted via EPR (Einstein-Podolsky-Rosen) paradox [5].

Keywords: `Randorm bit generator, CHSH inequality, Loophole`

1. Introduction

In recent years, there have been a number of experiments claiming that entanglement phenomenon can be exhibited at the classical level [4, 6, 7, 8, 9]. In a previous work in this journal, Bennett and Brassard [5] have used a coin toss model to argue that the so-called "EPR paradox"[10, 11, 12] can transform maximally entangled (secure) states in classically (weakly) correlated system. In this connection, we have also shown the equivalence in classical and quantum one-way functions [13]. Here, we use a coin toss experiment to show by means of a logic gates framework that the classical limit, *de facto*, passes into the quantum domain, making classic and quantum systems deducible from each other. This logical loophole can make cryptography systems based on quantum entanglement vulnerable to an opponent with low computing power.

2. Logical loophole

Let $E_1 = \{1, 1, 1\}$, $E_2 = \{1, 1, 0\}$, $E_3 = \{1, 0, 1\}$, $E_4 = \{1, 0, 0\}$, $E_5 = \{0, 1, 1\}$, $E_6 = \{0, 1, 0\}$, $E_7 = \{0, 0, 1\}$ and $E_8 = \{0, 0, 0\}$ be events of a straightforward probability experiment, where a coin is flipped three times, such that 0 represents tail, and 1 represents head for example, as shown in Fig.1.

Email address: `alexandre.castro@embrapa.br` (Alexandre de Castro)

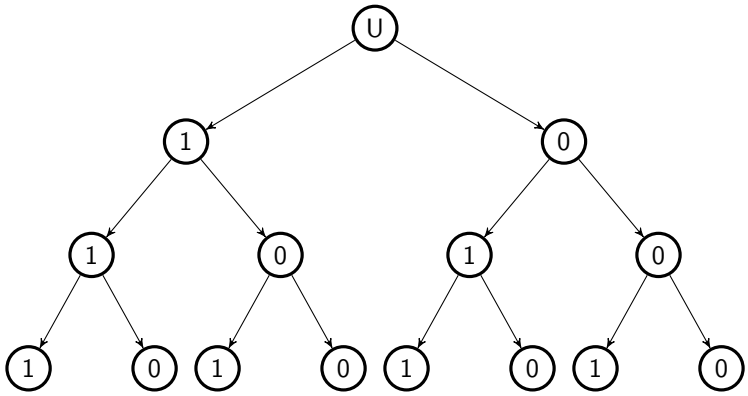


Figure 1: Random 3-bit sequence generation corresponds to flipping a coin three times, where the universal set $U = \{0, 1\}$ represents "head" and "tail". The third and second tossings are reduced to a single coin toss, which can result in either heads or tails, but not both.

Consider the sum of cardinalities given by Wigner's inequality $|E_3| + |E_4| \leq |E_3| + |E_4| + |E_2| + |E_7|$ [14, 15],[16, pp. 227-229]. Then, the cardinality of sum $|E_3 + E_4| \leq |E_3 + E_4 + E_2 + E_7|$ holds, since E_i is non-negative. These events are mutually exclusive, and if two events are mutually exclusive, then the XOR function can be used to describe their outcome. Therefore, $|\{1, 0, 1\} \oplus \{1, 0, 0\}| \leq |\{1, 0, 1\} \oplus \{1, 0, 0\} \oplus \{1, 1, 0\} \oplus \{0, 0, 1\}|$, hence, $|\{0, 0, 1\}| \leq |\{1, 1, 0\}|$.

Theorem 1. *Schröder-Bernstein theorem If* $|A| \leq |B|$ *and* $|B| \leq |A|$*, then* $|A| = |B|$ *(See proof in [17]).*

Remark 1. The sets $\{0, 0, 1\}$ and $\{1, 1, 0\}$ represent two complementary events, hence, there exists a bijection between them and, as a result, they have the same cadinality $|\{0, 0, 1\}| = |\{1, 1, 0\}|$. Consequently, the inequality $|\{0, 0, 1\}| \leq |\{1, 1, 0\}|$ is inverted by Schröder-Bernstein theorem. It follows that $|\{0, 0, 1\}| \geq |\{1, 1, 0\}|$.

Notice that the event $\{0, 0, 1\}$ can be represented by bit string $001_2 := 1_{10}$, and the decimal $1_{10} := x \oplus NOT(x)$ for $x = \{0, 1\}$. So, as a result of the Schröder-Bernstein theorem, we have $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$. The exclusive disjunction $x \oplus NOT(x)$ is equal to $(x \wedge x) \oplus NOT(x)$, and taking into account that the XOR operation is assumed as addition ($\oplus \to +$), the conjunction AND corresponds to multiplication ($x \wedge x = x \cdot x = x^2$), and the negation $NOT(x)$ can be replaced with the complement $1 - x$, we have that $x \oplus NOT(x)$ can be written as a two-valued logic $x \oplus NOT(x) := x^2 + 1 - x$. Taking the inequality constraint $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$, we obtain the multi-valued logic $|x^2 + 1 - x| \leq 1_{10}$ for $x \in [0, 1]$ such that $1_{10} := |x \oplus NOT(x)|$ for $x = \{0, 1\}$, where the Boolean domain $\{0, 1\}$ and the unit interval $[0, 1] = \{0, 1\} \cup (0, 1)$ are the two feasible regions satisfying problem's constraints. It follows that the fuzzy domain can still be narrowed down, since we must consider that the maps

$[0,1] \to (0,1)$ and $(0,1) \to [0,1]$ are both injective, which leads to existence of an isomorphism between $(0,1)$ and unit interval $[0,1]$.

Lemma 2. $(0,1) \sim [0,1]$

Proof. We can define a bijection $f : (0,1) \to \mathbb{R}$ by $f(x) = \tan(\pi x - \frac{\pi}{2})$, and the set of real numbers $\mathbb{R}$ has the same number of points as the line segment of length 1. As there are one-to-one correspondences between $(0,1)$ and $\mathbb{R}$, and between $\mathbb{R}$ and the unit interval $[0,1]$, then there is an isomorphism between $(0,1)$ and $[0,1]$.

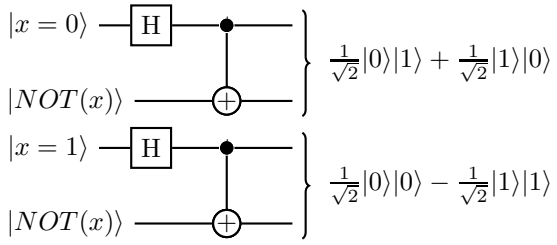
Remark 2. Isomorphic domains may be considered the same as long as one considers only their properties. Therefore, $[0,1]$ is replaced with $(0,1)$ and, consequently, the inequality constraint $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$ is reduced to $|x^2 + 1 - x| < 1_{10}$ for $x \in (0,1)$ such that $1_{10} = |x \oplus NOT(x)|$ for $x = \{0,1\}$.

The exclusive disjunction $x \oplus NOT(x)$ represents two spatially separated particles by a Hamming distance equal to 1, then two maximally entangled Bell states, $|\Psi^+\rangle$ and $|\Phi^-\rangle$, can be constructed.

Definition 1.

$$Let |x\rangle_{x=0,1} \xrightarrow{H} \frac{1}{\sqrt{2}}[(-1)^x|x\rangle + |1-x\rangle] \text{ be the Hadamard gate of a one} - \text{qubit register given by the size} - 2 \text{ (discrete Fourier transform) DFT.}$$

Remark 3. Then, the following quantum circuits evolve the input values, $x = \{0,1\}$, into two maximally entangled states of two qubits via controlled-NOT gate:



Therefore, the sum of correlation is equal to $2|x \oplus NOT(x)|_{x=0,1} := \frac{1}{\sqrt{2}}||00\rangle + |01\rangle + |10\rangle - |11\rangle|$ and, as a result $|x \oplus NOT(x)| = |\frac{1}{2}S_{CHSH}|$, where $|S_{CHSH}| = \frac{1}{\sqrt{2}}||00\rangle + |01\rangle + |10\rangle - |11\rangle|$. Considering that $|x^2 + 1 - x| < 1_{10}$ for $x \in (0,1)$ such that $1_{10} = |x \oplus NOT(x)|$ for $x = \{0,1\}$, and that $\lim_{L \to 1} L = 1$ where $L = |x^2 + 1 - x|$, then, we directly obtain that the number of elements (cardinality) of the open interval $(0,1)$ is $|S_{CHSH}| > 2$.

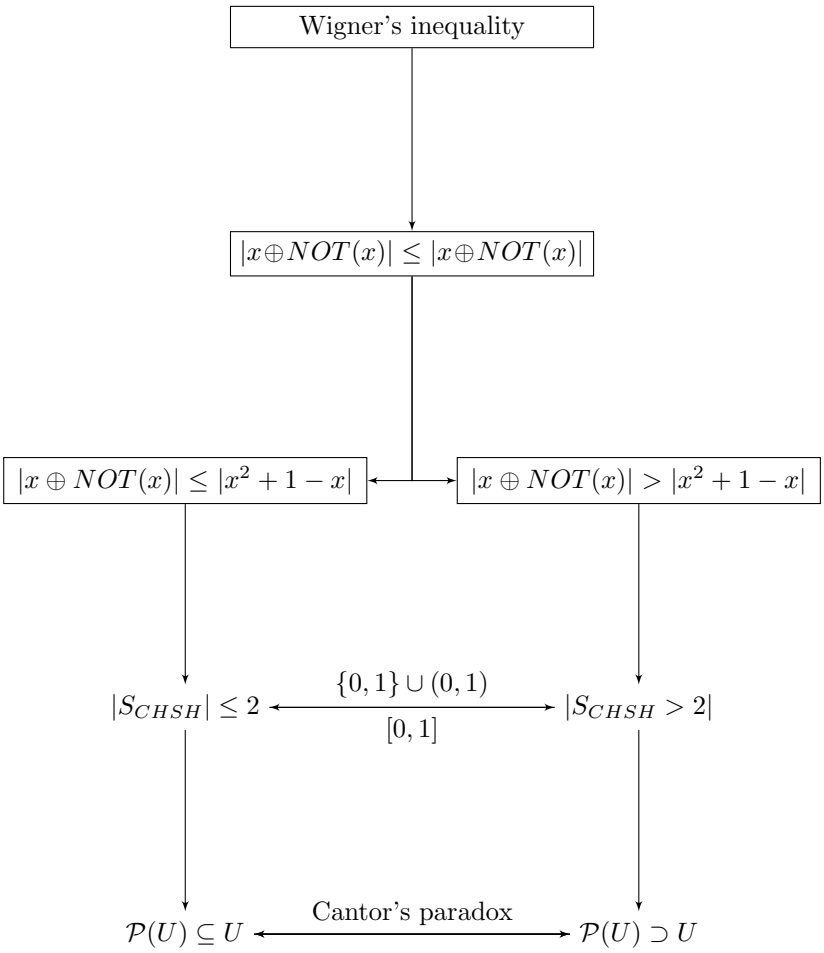


Figure 2: Information theoretic framework for an experiment like Bell test. The diagram shows the reduction of Wigner's inequality to Cantor's paradox via logic gates. Although the sets $\{0,1\}$ and $(0,1)$ are mutually exclusive, the bounds $|S_{CHSH}| \leq 2$ and $|S_{CHSH}| > 2$ are obtained from the same inequality constraint $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$ that in its turn corresponds to a Wigner's information-theoretic framework of a random experiment. Notice that the sample space shown in Fig. 1 is reduced to $\{0,1\}$, then the powerset, $\mathcal{P}(U)$, of the set all possible outcomes, U, of the experiment is equal to $\{\emptyset, \{0\}, \{1\}, \{0 \cup 1\}\}$, where $\emptyset$ becomes 0 over Boolean domain. As the events (0 or else 1) are mutually exclusive, then, the powerset can be reduced to $\mathcal{P}(U) = x \oplus NOT(x)$ for $x = \{0,1\}$. Rembembering from set theory that the union of the elements of $\mathcal{P}(U)$ is equal to the universal set U, hence, we have $\cup\mathcal{P}(U) = 0 \vee 1$[1] $= 1$. Thereby, $|x \oplus NOT(x)| \leq 1$ and $|x \oplus NOT(x)| > 1$, where $|x \oplus NOT(x)| = |\frac{1}{2}S_{CHSH}|$. As a result, $|P(U)| \leq |U|$ and $|\mathcal{P}(U)| > |U|$, which is the set-theoretic form of Cantor's paradox.

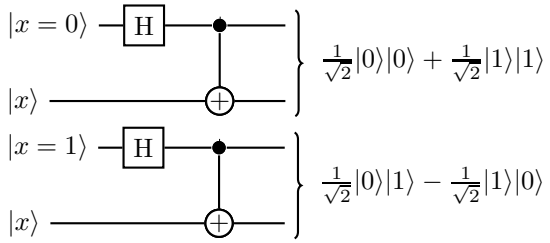
[1] Verify in the computational knowledge engine that $0 \vee 1$ is a universal set: `https://www.wolframalpha.com/input/?i=0+or+1`.

However, $|x^2+1-x| = |x \oplus NOT(x)|$ for $x = \{0,1\}$ and $|x^2+1-x| \leq 1_{10}$ for $x \in [0,1]$ such that $1_{10} := |x \oplus NOT(x)|$ for $x = \{0,1\}$, then, by antisymmetry, $|x^2+1-x| \geq |x \oplus NOT(x)|$, where $|x^2+1-x|$ is the lenght of the line segment $[0,1]$. Consequently, the number of elements of the Boolean domain $\{0,1\}$ is $|S_{CHSH}| \leq 2$. Therefore, this information-theoretic framework of Wigner's inequalty $|E_3|+|E_4| \leq |E_3|+|E_4|+|E_2|+|E_7|$ provides a loophole in the CHSH inequality, which reconciles it with the continuum hypothesis states that the set of real numbers has minimal possible cardinality which is greater than the cardinality of the set of integers, namely, $|S_{CHSH}| > 2$ such that $2 \geq |S_{CHSH}|$. This result shows that classical and quantum share the same bounds, once both conditions $|S_{CHSH}| \leq 2$ and $|S_{CHSH}| > 2$ hold from the same inequality constraint. Fig.2 shows the diagram of the reduction of the coin tossing experiment to a loophole in the CHSH inequality. The intervals $\{0,1\}$ and $(0,1)$ are mutually exclusive. However, both are present at once in the experiment. Namely, both conditions $|S_{CHSH}| \leq 2$ and $|S_{CHSH}| > 2$ are obtained from the same inequality constraint that represents the sample space of the experiment. This contradiction shows that Wigner's information-theoretic inequality is incompatible with axiomatic set theory, being able to exist only in a naïve set theory. Then, the probability interpretation of quantum mechanics, as used in information theory, is inconsistent with axiomatic set theory. For a concise idea, see the summary below:

Summary

Given Wigner's inequality $|E_3+E_4| \leq |E_3+E_4+E_2+E_7|$ for the mutually exclusive events $E_1 = \{111\}, E_2 = \{110\}, E_3 = \{101\}, E_4 = \{100\}, E_5 = \{011\}, E_6 = \{010\}, E_7 = \{001\}, E_8 = \{000\}$, we have that the inequality $|\{101\} \oplus \{100\}| \leq |\{101\} \oplus \{100\} \oplus \{110\} \oplus \{001\}|$ holds. Hence, we can write that $|\{001\}| \leq |\{110\}|$, where $\{001\}$ is complement of $\{110\}$. Then, $\{001\}$ and $\{110\}$ have the same cardinality, $|\{001\}| = |\{110\}|$. Consequently, $|\{001\}| \leq |\{001\}$, and remembering that $\{001\}_2 := 1_{10} = x \oplus NOT(x)$ for $x = \{0,1\}$, it follows that $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$, since every real number $\in [0,1]$ is less than or equal to itself (reflexivity). Algebraically, the exclusive disjunction $x \oplus NOT(x) = (x \wedge x) \oplus NOT(x)$ is equal to $x \cdot x + 1 - x = x^2 + 1 - x$ over the fuzzy domain. Then, we can transform the inequality $|x \oplus NOT(x)| \leq |x \oplus NOT(x)|$ in two parts: $|1| \leq |x^2+1-x|$ for the Boolean domain $x = \{0,1\}$, since every integer number is less than or equal to itself, and $|1| > |x^2+1-x|$ for the open interval $x \in (0,1)$, where $(0,1) \cup \{0,1\} = [0,1]$. Notice that $|1| = |\frac{1}{2} S_{CHSH}|$, where S_{CHSH} is the classical bound 2. So, $|\frac{1}{2} S_{CHSH}| \leq |x^2+1-x|$ and $|\frac{1}{2} S_{CHSH}| > |x^2+1-x|$. Considering that $Lim_{L \to 1} L = 1$, where $L = |x^2+1-x|$, we have that $|S_{CHSH}| \leq 2$ and $|S_{CHSH}| > 2$ over the continuum $[0,1]$. Thereby, the classical limit passes into the quantum domain, making classic and quantum systems share the same bounds.

It is not hard to see why this contradiction occurs, once classical and quantum are deducible from each other. Rember that the correlation function of spatially separated particles by a Hamming distance equal to 1 can be represented by the logic gate $x \oplus NOT(x)$ that outputs always 1 for $x = \{0, 1\}$. Therefore, by symmetry, $x \oplus NOT(x) \oplus 1 = 1 \oplus 1$, where $NOT(x) \oplus 1 = x$ for $x = \{0, 1\}$. Hence, from the nonlocal model $x \oplus NOT(x)$, we can obtain the model $x \oplus x$, whose Hamming distance between bits is equal to 0. Indeed, this result holds because from the local model $x \oplus x$ we can construct the Bell maximally entangled states $|\Phi^+\rangle$ and $|\Psi^-\rangle$:



This shows that the entanglement phenomenon can be exhibited at the classical level, in accordance with recent experimental outcomes [4, 6, 7, 8, 9], which can become quantum cryptography systems critically vulnerable to an opponent with low computing power.

References

[1] Clauser, J.F., Horne, M.A., Shimony, A., Holt, R.A. Proposed experiment to test local hidden-variable theories. Physical Review Letters, Vol. 23, pp. 880-884 (1969).

[2] Bell, J.S. Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press, UK (1987).

[3] Brassard, G. Methot, A.A., Strict hierarchy among Bell Theorems. Theoretical Computer Science. Vol. 486, pp. 4-10 (2013).

[4] Frustaglia, D. et al. Classical physics and the bounds of quantum correlations. Phys. Rev. Lett. 116, 250404 (2016).

[5] Bennett, C.H., Brassard, G. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science. Vol. 560(1) pp. 7-11 (2014).

[6] Toppel, A., Marquardt, F., Giacobino, C., Leuchs, E. Quantum-like nonseparable structures in optical beams. New J. Phys. 17, 043024 (2015).

[7] McLaren, M., Konrad, T., Forbes, A. Measuring the nonseparability of vector vortex beams. Phys. Rev. A 92, 023833 (2015).

[8] Qian, X.F., Little, B., Howell, J. C., Eberly, J. H. Shifting the quantum-classical boundary: theory and experiment for statistically classical optical fields. Optica 2, 611 (2015).

[9] Balthazar, W. F. et al. Tripartite nonseparability in classical optics. Opt. Lett. 41, 5797 (2016).

[10] Einstein, A; B Podolsky; N Rosen. Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" Physical Review. 47 (10): 777780 (1935).

[11] Nieuwenhuizen, T.M, Spicka, V, Aghdami, M.J., Khrennikov, A.Y. (eds). Beyond the Quantum. World Scientific, USA (2007).

[12] Hess, K. Einstein Was Right! CRC Press, Boca Raton (2015).

[13] de Castro, A. Quantum one-way permutation over the finite field of two elements. Quantum Information Processing. 16:149 (2017).

[14] Wigner, E.P. On Hidden Variables and Quantum Mechanical Probabilities. Am J. Phys., vol. 38: 1005-1015 (1970).

[15] d'Espagnat, B. The Quantum Theory and Reality. Scientific American, pp.158-167 (1979).

[16] Sakurai, J.J. Modern Quantum Mechanics. AddisonWesley, USA (1994).

[17] Hinkis, A. Proofs of the Cantor-Bernstein theorem. A mathematical excursion, Science Networks. Historical Studies 45, Heidelberg: Birkhuser/Springer (2013).