CONTROLLED-NOT FUNCTION CAN PROVOKE BIASED INTERPRETATION FROM BELL'S TEST EXPERIMENTS

ALEXANDRE DE CASTRO

ABSTRACT. Recently, we showed that the controlled-NOT function is a permutation that cannot be inverted in subexponential time in the worst case [Quantum Information Processing. 16:149 (2017)]. Here, we show that such a condition can provoke biased interpretations from Bell's test experiments.

Let $CNOT$ be the canonical two-qubit entangling gate in quantum key distribution (QKD) cryptographic protocols, where $CNOT|a, x\rangle = |a, a + x\rangle$, so that the control parameter a and the target variable $x \in F_2 = \{0, 1\}$.

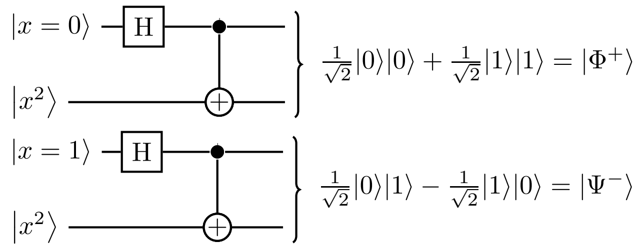
For $x = a$, $CNOT|a, x\rangle = |a, x^2 + x\rangle$, since $x \wedge x = x = x^2$, and for $x \neq a$, $CNOT|a, x\rangle = |a, x^2 + x + 1\rangle$, since $\neg x = x + 1 = x \wedge x + 1 = x^2 + 1$ [1]:

(i) The permutation $x^2 + x = x \oplus x$ is a factorable polynomial (reducible) over a finite field of two elements, whose Hamming distance between its even inputs is equal to 0 (local model), and (ii) The permutation $x^2 + x + 1 = x \oplus NOT(x)$ is a nonfactorable polynomial (irreducible) over a finite field of two elements, whose Hamming distance between its odd inputs is not equal to 0 (nonlocal model). However, these models are deducible from each other because $x^2 + x\ (+1) = 0\ (+1) = x^2 + x + 1$ and $x^2 + x + 1\ (+1) = 1\ (+1) = x^2 + x$ [1].

Consider the Hadamard basis $\{|+\rangle, |-\rangle\}$ of a one-qubit register given by:

$$|x\rangle_{x=0,1} \xrightarrow{H} \frac{1}{\sqrt{2}}[(-1)^x|x\rangle + |1 - x\rangle].$$

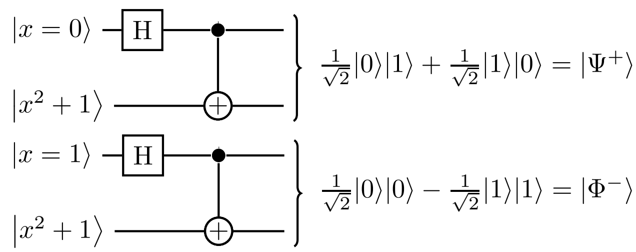
The circuit below takes computational basis $F_2 = \{0, 1\}$ to Bell states:



GRUPO DE COMPUTAÇÃO CIENTÍFICA, CENTRO NACIONAL DE PESQUISA TECNOLÓGICA EM INFORMÁTICA PARA A AGRICULTURA, EMPRESA BRASILEIRA DE PESQUISA AGROPECUÁRIA, CAMPINAS-SP BRAZIL 13083-886.

E-mail address: alexandre.castro@embrapa.br.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.3302v1 | CC BY 4.0 Open Access | rec: 29 Sep 2017, publ: 29 Sep 2017



Entangled states of two qubits known as the Bell states occur in conjugate pairs. Quantum states which are conjugates of each other have the same absolute value.

Hence,

$|x^2+x| = |\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle| =$

$= |\frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{2}}|1\rangle|1\rangle| = |x^2+x+1|$ and

$|x^2+x| = |\frac{1}{\sqrt{2}}|0\rangle|1\rangle - \frac{1}{\sqrt{2}}|1\rangle|0\rangle| =$

$= |\frac{1}{\sqrt{2}}|0\rangle|1\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle| = |x^2+x+1|$.

Therefore, $|x^2+x| = |x^2+x+1|$, since these models are deducible from each other. Notice that we can map the elements of the Hadamard basis to the computational basis using the group homomorphism $\{+1,-1,\times\} \mapsto \{0,1,+\}$ so that its inverse is also a group homomorphism.

Then, the exclusive disjunction x^2+x+1 over F_2 can be rewritten as $x + NOT(x) := X'\wedge\neg X''$, once the field's multiplication operation corresponds to the logical AND operation over the field of two elements. It is not difficult to see that for $X' = X'' = X'''$, $X'\wedge\neg X' = (X'\vee X''\vee X''')\wedge(\neg X'\vee\neg X''\vee\neg X''')$ can be written as a conjunctive normal form, $(X'\vee X''\vee X''')\wedge(X'\vee X''\vee\neg X''')\wedge(X'\vee\neg X''\vee X''')\wedge(X'\vee\neg X''\vee\neg X''')\wedge(\neg X'\vee X''\vee X''')\wedge(\neg X'\vee X''\vee\neg X''')\wedge(\neg X'\vee\neg X''\vee X''')\wedge(\neg X'\vee\neg X''\vee\neg X''')$ corresponding to the universal set $\{X', X'', X'''\}$ as shown in the following framework.

Suppose that we take a particle in the state X and subjected to three tests with two possible outcomes. (This is equivalent to three $spin$1/2 subsystems). We will call a first test X', a second test X'' and a third test X''', and label the outcomes *pass* and *fail* in accordance with Fig. 1 below.

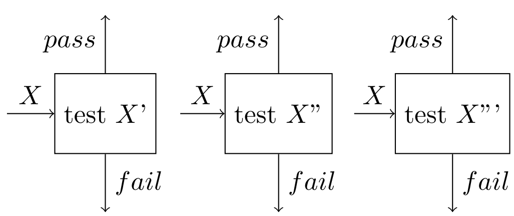


FIGURE 1. This simple experiment can also be seen as a straightforward probability problem, where we are going to flip a coin three times, so that 0 represents *tail*, and 1 represents *head*.

There are 8 possible outcomes of these three tests using 0 and 1 to represent *fail* and *pass* over a finite field of two elements.

Let Ω be the universal set $\{X', X'', X'''\}$, then all 8 possible different outcomes are represented by its subsets:
$\{\emptyset\} = \{000\}$,
$\{X'\} = \{100\}$,
$\{X''\} = \{010\}$,
$\{X'''\} = \{001\}$,
$\{X', X''\} = \{110\}$,
$\{X', X'''\} = \{101\}$,
$\{X'', X'''\} = \{011\}$,
$\{X', X'', X'''\} = \{111\}$.

The following elements shown in Table 1 are equivalent representations of the same value over a finite field of two elements [2, p. 134]:

Table 1. Polynomial representation $Poly(x)$ for all the mutually exclusive (8) possibilities of experiment. Set theory is isomorphic to Boolean Algebra.

Tests X',X$''$,X'''	Poly(x)	Probability
111	$x^2 + x + 1$	$\mathcal{P}r_1$
110	$x^2 + x$	$\mathcal{P}r_2$
101	$x^2 + 1$	$\mathcal{P}r_3$
100	x^2	$\mathcal{P}r_4$
011	$x + 1$	$\mathcal{P}r_5$
010	x	$\mathcal{P}r_6$
001	1	$\mathcal{P}r_7$
000	0	$\mathcal{P}r_8$

In third column of Table 1, $\mathcal{P}r_i$, with $i = 1, ...8$, is the probability of a specific outcome occurring in the sample space including all possible outcomes.

The probabilities $\mathcal{P}r_i$ are nonnegative, and therefore $\mathcal{P}r_3 + \mathcal{P}r_4 \leq \mathcal{P}r_3 + \mathcal{P}r_4 + \mathcal{P}r_2 + \mathcal{P}r_7$ within the framework conceived by Wigner [3, 4, 5], as described in detail in [6, p. 227-228]. (If we assume, with Wigner, the existence of these probabilities, his inequality must be true, because the existence of these probabilities corresponds in essence to Kolmogorov's consistency conditions).

Let an event E_i be a set of the outcomes of experiment, i.e, a subset of the sample space Ω. If each outcome in the sample space Ω is equally likely, then the probability that event E_i occurs is $\mathcal{P}r_i = \frac{|E_i|}{|\Omega|}$, where the bars $|\cdot|$ denote the cardinality of sets. As each bit string can be written as a polynomial over a finite field of two elements, then the cardinality of Ω, and for each E_i, is the modulus of a polynomial. Hence, $|x^2 + 1| + |x^2| \leq |x^2 + 1| + |x^2| + |x^2 + x| + |1|$, because $|\Omega| = 1$, since the universal set $x^2 + x + 1 = 1$ for $x = \{0, 1\}$. Consequently, $|x^2 + 1 + x^2| \leq |x^2 + 1 + x^2 + x^2 + x + 1|$, once the all polynomials are nonnegative.

Considering that field's multiplication corresponds to the logical AND, then $x^2 = x$, since $x \wedge x = x$. Hence, $|x^2 + 1 + x| \leq |x + 1 + x + x^2 + x + 1|$.

Rearranging this inequality, we get $|x^2 + x + 1| \leq |x^2 + x|$, because the field's addition operation $x + x = 0$ corresponds to the logical XOR operation. Notice that the polynomial $x^2 + x = NOT(x^2 + x + 1)$ for $x = \{0, 1\}$. Therefore, $|x^2 + x + 1| \leq |1 - (x^2 + x + 1)|$ since, algebraically, the negation $NOT(x^2 + x + 1)$ is replaced with complement $1-(x^2+x+1)$. Hence, $|x^2+x+1| \leq 1-|x^2+x+1|$ because $0 \leq x^2+x+1 \leq 1$.

It is straightforward to see that $|x^2+x+1| \leq \frac{1}{|x^2+x+1|}$, consequently, $\frac{1}{|x^2+x+1|} \leq 1-\frac{1}{|x^2+x+1|}$, where $\frac{1}{|x^2+x+1|} = \left(\frac{1}{|x^2+x+1|}\right)^2$.

As a result,

$$\left(\frac{1}{|x^2+x+1|}\right)^2 \leq 1-\frac{1}{|x^2+x+1|} \tag{1}$$

The polynomial x^2+x+1 over a finite field with a characteristic 2 corresponds to the exclusive disjunction $x \oplus NOT(x)$, where $NOT(x) = x^2 \oplus 1$ for $x = |0\rangle$ or $x = |1\rangle$.

Therefore:

$$|+\rangle = \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}+1\\+1\end{pmatrix}$$
$$|-\rangle = \begin{pmatrix}1\\0\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}+1\\-1\end{pmatrix},$$

so that $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, where the normalizing constant $\frac{1}{\sqrt{2}}$ was omitted. This logical operation can also be regarded as the Fourier transform [7, p. 50] on the Galois field of two elements $H_2|x\rangle_{x=\{0,1\}} = |\pm\rangle$, where $H_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$ is the Hadamard matrix of order 2.

Fig. 2 depics the Hadamard basis $\{|+\rangle, |-\rangle\}$ of a one-qubit register on the Hilbert space. Notice that the ratio $\frac{1}{|x^2+x+1|}$ in Ineq. 1 corresponds to $\sin 45°$ over $\mathbb{R}^2$, since the vectors with coordinates $(+1, \pm 1)$ have the same direction as the unit vectors $\frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle$ that make half a right angle with the axes in the plane. Hence, Ineq. 1 stays $(\sin\theta)^2 \leq 1-\sin\theta$ for $\theta = 45°$.

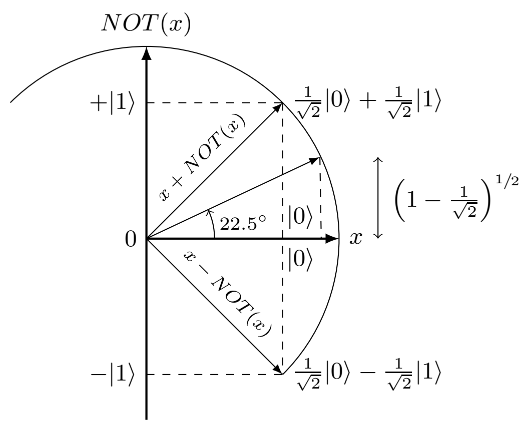


FIGURE 2. The Hadamard gate operates as a reflection around $= \frac{\pi}{8}$ that maps the x-axis to the 45° line, and the $NOT(x)$-axis to the −45° line.

Consider the trigonometric identity $|\sin\left(\frac{\theta}{2}\right)| = \left(\frac{1-\cos(\theta)}{2}\right)^{1/2}$. Then, the equality $1-\sin\theta = 2(\sin\frac{\theta}{2})^2$ holds, since $\cos\theta = \sin\theta$ for $\theta = 45°$. Consequently, $(\sin 45°)^2 \leq 2(\sin 22.5°)^2$.

Rearranging this last inequality, we get:

$$\frac{1}{2}(\sin 45°)^2 \leq \frac{1}{2}(\sin 22.5°)^2 + \frac{1}{2}(\sin 22.5°)^2, \tag{2}$$

that is the inequality obtained by Bell is his paper [6, p. 230][8], where 45° and 22.5° are Bell test angles, these being the ones for which the quantum theory gives the greatest violation of the inequality, i.e., $0.2500 \leq 0.1464$(i).

Remember that $\{X', X"\}$ is a subset of the universal set $\{X', X", X"'\}$, hence, the cardinality of subset $\{X', X"\}$ is less than or equal to the cardinality of set $\{X', X", X"'\}$. Then, obviously, the inequality $|x^2+x| \leq |x^2+x+1|$ holds. (If we trust standard set theory, this axiomatic inequality has to be true).

So, Ineq. 1 is reversed:

$$\frac{1}{2}(\sin 45°)^2 \geq \frac{1}{2}(\sin 22.5°)^2 + \frac{1}{2}(\sin 22.5°)^2, \tag{3}$$

as opposed to Ineq. 2. Consequently, $0.2500 \geq 0.1464$(ii).

The inequalities (i) and (ii) exist at once for Bell test angles, which shows that there is an ambiguity in axiomatic set theory on which Wigner [3] relied to derive a general form of Bell's inequalities. As a consequence, we have that $|x^2+x| \leq |x^2+x+1|$ and $|x^2+x+1| \leq |x^2+x|$, where $2|x^2+x+1|_{x=\{0,1\}} = \frac{1}{\sqrt{2}}(||01\rangle + |10\rangle| + ||00\rangle - |11\rangle|)$, so that:

$$|[x \oplus NOT(x)]_{x=0}| \mapsto \quad \frac{1}{\sqrt{2}}||0\rangle|1\rangle + |1\rangle|0\rangle|$$

$$|[x \oplus NOT(x)]_{x=1}| \mapsto \quad \frac{1}{\sqrt{2}}||0\rangle|0\rangle - |1\rangle|1\rangle|$$

As the set x^2+x+1 is a subset of itself, hence, $|x^2+x+1| \leq |x^2+x+1|$. It follows that the conditions $|x^2+x+1| \leq 1$ and $|x^2+x+1| > 1$ hold. Consequently, $\frac{1}{2\sqrt{2}}(||01\rangle + |10\rangle| + ||00\rangle - |11\rangle|) \leq 1$ and $\frac{1}{2\sqrt{2}}(||01\rangle + |10\rangle| + ||00\rangle - |11\rangle|) > 1$.

Defining $\frac{1}{\sqrt{2}}(||01\rangle + |10\rangle| + ||00\rangle - |11\rangle|)$ as a sum of correlations S, we have $S \leq 2$ and $S > 2$ at once, which shows that the number 2 cannot be used as separability criterion. As a result of this logical hole, the problem to determine whether a given state is entangled or classically correlated is undecidable via CHSH inequality [9, 10], i.e, $2 < ||00\rangle + |01\rangle + |10\rangle - |11\rangle| \leq 2$, which can provoke interpretation bias in Bell's test experiments for quantum key distribution (QKD) cryptographic protocols.

References

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

[2] Stalling, W. Cryptography and Networks Security. Principles and Practice. Prentice Hall, NY (2011).

[3] Wigner, E.P. Am J. Phys., vol. 38: 1005-1015 (1970).

[4] Castelletto, S., Degiovanni, I.P., Rastello, M.L. A Modified Wigners Inequality for Secure Quantum Key Distribution. Phys. Rev. A 67, 044303 (2003).

[5] Home, D. Saha, D., Das, S. Multipartite Bell-type inequality by generalizing Wigner's argument. Phys. Rev. A 91, 012102 (2015).

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.3302v1 | CC BY 4.0 Open Access | rec: 29 Sep 2017, publ: 29 Sep 2017

[6] Sakurai, J.J. Modern Quantum Mechanics. AddisonWesley, USA (1994).
[7] Amoroso, R.L. Universal Quantum Computing. World Scientific Publishing, USA (2017).
[8] Bell, J.S. Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press, UK (1987).
[9] Clauser, F., Horne, M.A., Shimony, A. Holt, R.A. Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett., 23 (15): 8804 (1969).
[10] Nielsen, M.A., Chuang, I.L. Quantum Computation and Quantum Information (Cambridge University Press, 2010).