Quantum Entanglement, Bell’s Inequalities and Quantum Computation

Dharmine J. Jamnadas
dharmine.jamnadas@tecnico.ulisboa.pt
Instituto Superior Técnico, Universidade Técnica de Lisboa, Portugal

***Abstract*—The main objective of this paper is to provide an overview of some quantum computation concepts.**

An important concept is the Quantum Nonlocality, which was introduced by an intriguing EPR (Einstein-Podolsky-Rosen) theoretical experiment. This concept was also explored in form of games like the PR (Popescu-Rohrlich) box, and GHZ (Greenberger–Horne–Zeilinger) game to emphasize the power of quantum mechanics. Bell’s contribution was fundamental to comprehend that the hidden value argument couldn’t be the explanation for the obtained results. This paper will explore those experiments and games assuring that quantum superposition and quantum entanglement are real by explaining them mathematically.

More complex quantum algorithms only make sense if it solves problems that classical computation algorithms cannot solve. And this is exactly what happens with the large number factorization problem, which today cannot be solved by classical computers and theoretically can be solved by quantum computers. Although this seems to be good, there are some inherent security risks, because today this difficulty is explored to make classical encryption code such as RSA (Rivest–Shamir–Adleman). This paper will also explain how Shor’s Algorithm (which solves the large factoring problem) could be used to break RSA encryption code.

***Index Terms*— Quantum Nonlocality, EPR Experiment, PR Boxes, GHZ Game, Quantum Computation, Shor’s Algorithm**

I. Introduction

The computer science field started with the theoretical study of algorithms (sequence of computational steps that transform a set of values which can be called input into other sets of values that are called output [1]). The classical computer science field was born in 1936 when Alan Turing [2] attempted to prove that mathematician David Hilbert’s decision problem (Entscheidungsproblem) solution was true. In this problem, David Hilbert believed that there was an algorithm that could tell if a proposition was universally valid, given all the axioms of math. Turing developed a model for computation (now known as the Turing machine) that proved Hilbert's decision problem was surprisingly not true. Later, Church–Turing thesis corroborated that any algorithm can be run in a Turing machine. Until this day, if an algorithm cannot be run in the Turing machine, then it’s not computable. In fact, even a Turing machine can be simulated in a (Universal) Turing machine.

Turing Machine is an abstract representation that defines the mathematical model of a computer and this was the first software representation of the computer field.

In 1945, von Neumann proposed a complementary theoretical architecture that would be the baseline to construct a classical computer. The innovation consisted in saving a program and its data in memory before writing the output [3]. The architecture proposed by Von Neumann is now used in all classical computers.

Von Neumann architecture contains the following components: a CPU (Central Processing Unit), a memory unit, an input and output devices.

In 1947, John Bardeen, Walter Brattain, and Will Shockley developed the transistor that helped computer hardware to grow rapidly [4]. The growth was so fast that in 1965, Gordon Moore stated that the computer power would increase once every two years, keeping the cost constant (Moore’s law) [5]. To increase power one needs to increase the number of transistors in a dense integrated circuit which leads to an increase in the number of components on a single silicon chip. However, this increase is not indefinitely sustainable. As the size of the chip approximates into atomic sizes, the laws of classical physics are challenged making it impossible to make more powerful computers. To overcome these challenges Richard Feynmann initiated a revolutionary thought. He stated that to simulate physical phenomenon’s it would be necessary to build quantum computers [6]. Before looking at the definition and specificities of quantum machines, it is relevant to notice that in 1985, David Deutsch introduced an important principle, the Church-Turing-Deutsch principle [7]. He showcased that all physical processes can be simulated through a Quantum Turing machine which consists in a generalization of the previously explained Universal Turing Machine.

Nowadays it is also known that quantum computers can be used beyond the simulation of physical phenomenons. Quantum computers can do very specific tasks such as searching in large datasets, assisting in drug development, and supporting traffic route optimization in a significantly shorter time when compared to classical computing. Even though it is true that quantum computers can perform all the tasks of classical computers, it is not true they should be used as a replacement. On one hand, quantum machines are extremely expensive and therefore industry scalability is not viable. On the other hand, using such machines to perform relatively simple (or not overly complex) tasks would not bring relevant gains or benefits for the user (the trade-off between the time saved and the resources/energy allocated to use the computer is not justified).

II. Quantum Nonlocality

Quantum Nonlocality was a very controversial principle when discovered. The topic is counterintuitive being Einstein the first person to find this intriguing.

A. *Einstein-Podolsky-Rosen thought experiment*

Quantum Nonlocality was and still is a counterintuitive principle because it indicates that one particle property can be influenced by a different particle in a faraway distance and this is made instantaneously (meaning in a velocity greater than the velocity of light).

This was so controversial, that Einstein claimed that properties of a particle in region B cannot be affected by properties of another particle on faraway region A, rejecting the so-called spooky actions at a distance [8]. Einstein advocated that each particle should have hidden values and these hidden values would explain the correlation between two separated particles in each region.

This hidden value argument started in a thought experiment made in 1935 by Einstein, Podolsky, and Rosen [9], but it was rejected mathematically by John Bell in 1964 [10] and later on (in the early 1980s) proved wrong experimentally by Alain Aspect [11].

1) *EPR's Device*

In this experiment, we have one device that produces two independent particles that go to opposite sides in each run. One goes to region A (Detector A) and the other to region B (Detector B). In each run, both particles collapse in different detectors with 3 different settings (1, 2 and 3) and the outcome will be one of the following light colors: Green or Red (G or R).

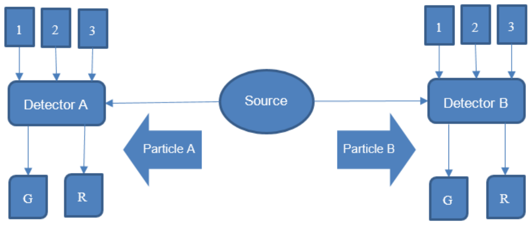


Figure 1: A schematic representation of the EPR device and its two detectors

After millions of runs, the two main conclusions were:

1. When both switches have the same setting, the outcome is always the same color;
2. The likelihood of the outcome being the same colors or different colors is equal

2) *Hidden Value Argument*

The hypothesis for explaining the correlation between colors of different regions was the hidden value proposition which stated that the particles have values before they leave the device. There are no links or communication between two particles after they leave the device (source). The detectors are also independent. Table 1 presents the possible outcomes (outputs) according to the inputs (settings) for each particle, once they collapse on each of their detectors.

Table 1: Individual outcomes and respective combination according to the configuration of settings 1, 2 and 3

1	2	3
G	G	G
G	G	R
G	R	G
G	R	R
R	G	G
R	G	R
R	R	G
R	R	R

The assumption is: the outcome for one particle has a hidden value associated to the combination of detector settings and the collapse of the particle. To check if there is any type of correlation between the setting and the light color, it is necessary to check the combination of settings of both detectors: $\{11; 12; 13; 21; 22; 23; 31; 32; 33\}$ and their individual outcomes$\{G; R\}$. By performing this analysis, conclusion 2. 'The likelihood of the outcome being the same colors or different colors is equal' will be tested.

Each run can be represented by {12GR} and this means that the setting in detector A is 1 and the outcome color is Green and the setting in detector B is 2 and the outcome color is Red.

In the first row of Table 1, we have (GGG) for any kind of setting (123), which means that the two particles (A and B) will flash the same color G in each run.

$$\{11GG; 12GG; 13GG; 21GG; 22GG; 23GG; 31GG; 32GG; 33GG\} \\ \rightarrow P_{hiddenvalue}(same\ color \mid GGG) = 9/9$$

Where $P_{hiddenvalue}(same\ color \mid GGG)$ can be read as the probability of flashing the same color knowing that the hidden value in setting 123 is GGG.

Probability of 1 means that all runs have the same color output.

In the last row of Table 1, we have (RRR) for any kind of setting (123), which means that the two particles (A and B) will flash the same color R in each run.

$$\{11RR; 12RR; 13RR; 21RR; 22RR; 23RR; 31RR; 32RR; 33RR\} \\ \rightarrow P_{hiddenvalue}(same\ color \mid RRR) = 9/9 = 1$$

(Probability of 1 means that all runs have the same color output).

For the second row we have (GGR) for setting (123), which means that the two particles (A and B) will flash the same color in some of the runs.

$$\{11GG; 12GG; 21GG; 22GG; 33RR\} \rightarrow P_{hiddenvalue}(same\ color \mid GGR) = 5/9.$$

Applying the same logic for the remaining rows of Table 1 one conclusion stands out:

$$P_{hiddenvalue}(Same\ color) \geq (5/9) \qquad (1)$$

This contradicts the conclusion from the earlier section (EPR's Device): 2. 'The likelihood of the outcome being the same colors or different colors is equal.'

Because If

$$P_{hiddenvalue}(Same\ color) + P_{hiddenvalue}(Different\ color) = 1 \qquad (2)$$

And

$$P_{hiddenvalue}(Same\ color) \geq 5/9 \qquad (3)$$

Then

$$P_{hiddenvalue}(Same\ color) \neq P_{hiddenvalue}(Diferent\ color) \qquad (4)$$

For this reason, Bell concludes that the hidden proposition cannot be true, meaning that there is no hidden value in each particle once they leave the source.

3) *Quantum Mechanics (QM) Argument*

If there is no hidden value in each particle before it leaves the source, a new hypothesis arises - both particles should be influenced by each other somehow and the particle does not have value until it collapses. This means that the particle is in superposition form before it collapses.

a) *Quantum Superposition*

To represent a particle, Dirac notation will be used (also known as bracket notation).

In this form, one particle is represented by ket $\mid \psi \rangle$:

$$\mid \psi \rangle = \alpha \mid 0 \rangle + \beta \mid 1 \rangle, \qquad \alpha, \beta \in \mathbb{C} \qquad (5)$$

Where α and β are the amplitudes with probabilities of $|\alpha|^2$ and $|\beta|^2$ being $|\alpha|^2 + |\beta|^2 = 1$.

In this particular example, $|0\rangle$ represents horizontally (→) polarized amplitude and $|1\rangle$ represents vertically (↑) polarized amplitude. If the particle is only represented by only one amplitude then the particle is vertically or horizontally polarized being the other amplitude 0.

b) *Quantum Entanglement*

Each particle has its properties. So particle A is represented with $\mid \psi \rangle_{\boldsymbol{A}}$ and Particle B with$\mid \psi \rangle_{\boldsymbol{B}}$

$$\mid \psi \rangle_{\boldsymbol{A}} = \alpha_A \mid 0 \rangle_{\boldsymbol{A}} + \beta_A \mid 1 \rangle_A, \qquad \alpha, \beta \in \mathbb{C} \qquad (6)$$

$$\mid \psi \rangle_{\boldsymbol{B}} = \alpha_B \mid 0 \rangle_{\boldsymbol{B}} + \beta_B \mid 1 \rangle_B, \qquad \alpha, \beta \in \mathbb{C} \qquad (7)$$

But when particles are entangled both states are inseparable, hence cannot be studied as separate states.

The final state is then, simply represented by:

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|00\rangle_{AB} + |11\rangle_{AB}\right] \qquad (8)$$

As there are three settings, this means that there are three types of polarization filters. Each filter is polarized at a very specific angle. If the angle of polarization of the particle is the same as the polarization filter the particle goes through the filter (the outcome is Green), otherwise it's blocked (the outcome is Red). The particle only defines its orientation once it collapses on the filter.

The three settings number are represented in Figure 2 by their respective angles of polarization. Each of the settings (1, 2 or 3) has two angles representation because they could have one of the two directions represented.

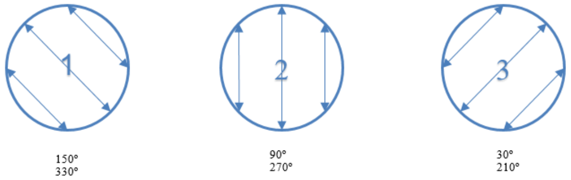


Figure 2:Settings numbers 1,2 and 3 and respective angles of polarization

According to the Malus Law, the probability of having the same outcome is given by:

$$P(\theta) = cos^2(\theta) \qquad (9)$$

$$\theta = \theta_B - \theta_A \qquad (10)$$

Where θ is the difference between the angle of particle B and particle A once they collapse the filter.

If the settings are the same {11;22;33} they will flash the same color because $P\ (0^o) = \cos^2(0^o) = 1$.

If the settings are different {12;13;21;23;31;32} the particles have the probability of flashing the same according to $P(\pm 300°) = P(\pm 240°) = P(\pm 120°) = P\ (\pm 60^o) = \cos^2(60^o) = 1/4$.

Which leads to

$$P_{QM}(Same\ color) = P(Same\ Setting).P(flashing\ same\ color\ |same\ setting) + P(Different\ Setting).P(flashing\ same\ color\ |Different\ Setting) \qquad (11)$$

$$P_{QM}(Same\ color) = \frac{3}{9}.1 + \frac{6}{9}.\frac{1}{4} = \frac{1}{3} + \frac{1}{6} = \frac{1}{2} \qquad (12)$$

Therefore, according to the quantum mechanics hypothesis, the outcome same colors in both detectors is as likely as different colors, not contradicting the EPR experiment.

$$P_{QM}(Same\ color) + P_{QM}(Different\ color) = 1 \qquad (13)$$

$$P_{QM}(Same\ color) = P_{QM}(Different\ color) = \frac{1}{2} \qquad (14)$$

B. Popescu-Rohrlich (PR) Box

Popescu and Rohrlich invented a theoretical device [12] that today is also known as PR boxes. These boxes are presented as game boxes to demonstrate one more time that the hidden value argument proposed by Einstein does not explain the results obtained in a subatomic world.

1) PR Device

In this thought experiment, we have one device very similar to the EPRs device. The PR device produces two independent photons in each run that goes to opposite sides. One goes to region A (Detector A) and the other goes to region B (Detector B). In each run, both photons collapse in different detectors with 2 different polarization filters (0, 1) and the outcome will be one of the following values: (0, 1).

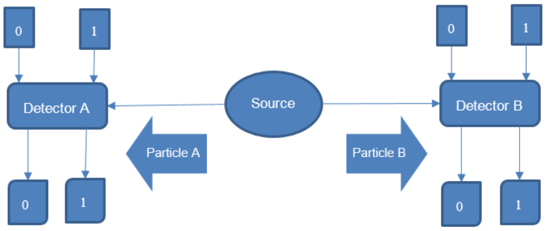


Figure 3: A schematic representation of the PR device and its two detectors

2) Hidden Value Argument

Table 2 shows the possible outcomes (outputs) according to the inputs (settings), for each particle, once they collapse on each of their detectors if a hidden values argument is used.

In the first two columns, the assumption is that both photons have a hidden polarization defined, once they leave the source and that this will define if the photon goes through or if it is blocked once it collapses on the polarization filter:

A. The Photon is always blocked by the polarization filter (independently of its value) meaning that the outcome value on the detector is always 0;
B. The Photon always passes by polarization filter (independently of its value) meaning that the outcome value on the detector is always 1;
C. The Photon is blocked or passes by a polarization filter according to the value of the polarization filter:
    - If the polarizer has a value of 0 the photon is blocked meaning that the outcome value on the detector is always 0;
    - If the polarizer has a value of 1 the photon passes, meaning that the outcome value on the detector is always 1;
D. The Photon is blocked or passes by a polarization filter according to the opposite value of the polarization filter:
    - If the polarizer has a value of 0 the photon passes, meaning that the outcome value on the detector is always 1;
    - If the polarizer has a value of 1 the photon is blocked, meaning that the outcome value on the detector is always 0.

The value x represents the value of the setting of detector A and y the value of the setting of detector B. Value a is the value of the outcome in detector A and b is the outcome value in detector B.

Table 2: Table of probabilities of scoring according to combination chosen

Photon A hidden's value	Photon B hidden's value	Results for x=0 and y=0	Results for x=0 and y=1	Results for x=1 and y=0	Results for x=1 and y=1	Probability of Scoring
A	A	a = 0;b = 0	a = 0;b = 0	a = 0;b = 0	a = 0;b = 0	$P_{hv}(Score) = \frac{3}{4}$
A	B	a = 0;b = 1	a = 0;b = 1	a = 0;b = 1	a = 0;b = 1	$P_{hv}(Score) = \frac{1}{4}$
A	C	a = 0;b = 0	a = 0;b = 1	a = 0;b = 0	a = 0;b = 1	$P_{hv}(Score) = \frac{3}{4}$
A	D	a = 0;b = 1	a = 0;b = 0	a = 0;b = 1	a = 0;b = 0	$P_{hv}(Score) = \frac{1}{4}$
B	A	a = 1;b = 0	a = 1;b = 0	a = 1;b = 0	a = 1;b = 0	$P_{hv}(Score) = \frac{1}{4}$
B	B	a = 1;b = 1	a = 1;b = 1	a = 1;b = 1	a = 1;b = 1	$P_{hv}(Score) = \frac{3}{4}$
B	C	a = 1;b = 0	a = 1;b = 1	a = 1;b = 0	a = 1;b = 1	$P_{hv}(Score) = \frac{1}{4}$
B	D	a = 1;b = 1	a = 1;b = 0	a = 1;b = 1	a = 1;b = 0	$P_{hv}(Score) = \frac{3}{4}$
C	A	a = 0;b = 0	a = 0;b = 0	a = 1;b = 0	a = 1;b = 0	$P_{hv}(Score) = \frac{3}{4}$
C	B	a = 0;b = 1	a = 0;b = 1	a = 1;b = 1	a = 1;b = 1	$P_{hv}(Score) = \frac{1}{4}$
C	C	a = 0;b = 0	a = 0;b = 1	a = 1;b = 0	a = 1;b = 1	$P_{hv}(Score) = \frac{1}{4}$
C	D	a = 0;b = 1	a = 0;b = 0	a = 1;b = 1	a = 1;b = 0	$P_{hv}(Score) = \frac{3}{4}$
D	A	a = 1;b = 0	a = 1;b = 0	a = 0;b = 0	a = 0;b = 0	$P_{hv}(Score) = \frac{1}{4}$
D	B	a = 1;b = 1	a = 1;b = 1	a = 0;b = 1	a = 0;b = 1	$P_{hv}(Score) = \frac{3}{4}$
D	C	a = 1;b = 0	a = 1;b = 1	a = 0;b = 0	a = 0;b = 1	$P_{hv}(Score) = \frac{3}{4}$
D	D	a = 1;b = 1	a = 1;b = 0	a = 0;b = 1	a = 0;b = 0	$P_{hv}(Score) = \frac{1}{4}$

In this table the $P_{hv}(Score|line\_combination)$ is calculated, similarly, in each line.

Bellow the example, where $line\_combination = AA$ (first line of the table)

$$P_{hv}(Score|AA) = \frac{Score_{AA\_Total}}{N_{AA\_Total}} \tag{15}$$

N_{AA_Total} is the number total of possible choices and $Score_{AA\_Total}$ is the sum of each score: $Score_{AA}(x = 0; y = 0), Score_{AA}(x = 0; y = 1), Score_{AA}(x = 1; y = 0)$ and $Score_{AA}(x = 1; y = 1)$. Each score value is calculated accordingly to Table 3

Table 3: Score Combination according to the input of Detector A (x_0, x_1) and B(y_0, y_1)

	x=0 (x_0)	x=1 (x_1)
y=0 (y_0)	If a=b, then score = 1 else score = 0	If a=b, then score = 1 else score = 0
y=1 (y_1)	If a=b, then score = 1 else score = 0	If a≠ b, then score = 1 else score = 0

In the remaining rows ($line\_combination \in \{AB, AC, AD, BA, BB, BC, BD, CA, CB, CC, CD, DA, DB, DC, DD\}$), the same logic of the first row is used ($line\_combination = AA$).

In conclusion :

$$P_{hiddenvalue}(Score) \leq 75\% \qquad (16)$$

This means that in the best case scenario it is possible to win the game 3 out of 4 times (75%) using the hidden value proposition.

3) *Quantum Mechanics (QM) Argument*

In the previous subchapter was demonstrated that the maximum probability of scoring (running a successful simulation) using the hidden value proposition was $\frac{3}{4}$. In this subchapter, the same probability will be calculated using the quantum mechanics proposition.

As seen in the EPRs subchapter, both photons are entangled and cannot be studied individually. They will leave the source in the following state.

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|00\rangle_{AB} + |11\rangle_{AB}\right] \qquad (17)$$

They are in a superposition state and the only thing that is possible to conclude before their collapse in their respective detectors is that they both have $\frac{1}{2}$ chances of collapsing as 0 (blocked) and $\frac{1}{2}$ chances of collapsing as 1 (passing through the polarizer). Both photons, A and B, will have the same polarization once they collapse on detectors. The outcome will be 0 or 1 according to the polarization of the filters settings on Detector A and Detector B.

In this example, polarization filters (represented by the settings) have different axes in both detectors. Detector A is represented by either $x = 0$ or $x = 1$ (with an angle of 45° between them). Detector B is represented by either $y = 0$ or $y = 1$(with an angle of 45° between them).

Figure 4 demonstrates the angle between axes of Detector A and B altogether.

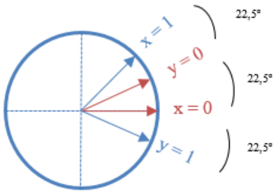


Figure 4: Polarization filter directions and angles between 4 different values of x and y

According to the Malus Law, the probability of having the same outcome is given by:

$$P_s = cos^2(\theta) \qquad (18)$$

$$\theta = \theta_B - \theta_A \qquad (19)$$

Where θ is the difference between the angle of particle B and particle A once they collapse the filter.

Following the same law, the probability of having a different outcome is given by:

$$P_d = \sin^2(\theta) \qquad (20)$$

$$\theta = \theta_B - \theta_A \qquad (21)$$

Referring back to Figure 4, if the combination of the settings in detector A and B are {00;01;10} then the probability of having the same outcome is given by $P_s\ (22{,}5^o) = \cos^2(22{,}5^o)$.

If the settings are {11} the probability of having the different outcome is $P_d\ (67{,}5^o) = \sin^2(67{,}5^o) = \cos^2(22{,}5^o)$.

This leads to:

$$\begin{aligned} P_{QM}(Score) = P(x_0;y_0).P(a = b\,|x_0;y_0) + P(x_0;y_1).P(a = b\,|x_0;y_1) \\ + P(x_1;y_0).P(a = b\,|x_1;y_0) \\ + P(x_1;y_1).P(a \neq b\,|x_1;y_1) \end{aligned} \qquad (22)$$

$$\begin{aligned} P_{QM}(Score) = \frac{1}{4}.\cos^2(22{,}5^o) + \frac{1}{4}.\cos^2(22{,}5^o) + \frac{1}{4}.\cos^2(22{,}5^o) \\ + \frac{1}{4}.\sin^2(67{,}5^o) \end{aligned} \qquad (23)$$

$$P_{QM}(Score) = \cos^2(22{,}5^o) = \frac{1}{4}(2 + \sqrt{2}) \approx 85\% \qquad (24)$$

In conclusion, we have a better probability of scoring using quantum mechanics preposition than using hidden values preposition.

$$P_{hiddenvalue}(Score) < P_{QM}(Score) \qquad (25)$$

C. *Greenberger–Horne–Zeilinger (GHZ) Game*

The Greenberger–Horne–Zeilinger (GHZ) experiment is another important experiment that explains nonlocality with an entanglement involving three particles. This leads to a new state (state of three entangled particles) proposed in 1989, by the article Bell's theorem without inequalities [13], in which statistical analysis is not required to contradict hidden variables theory, showing the accuracy of quantum mechanics argument.

1) *GHZ Device*

This device has a source that produces three photons, one goes to region A (Detector A), the second goes to region B (Detector B) and the third goes to region C (Detector C). In each run, three photons collapse in different detectors with 2 different polarization filters (X, Y) and the outcome will be one of the following values: (+1, -1).

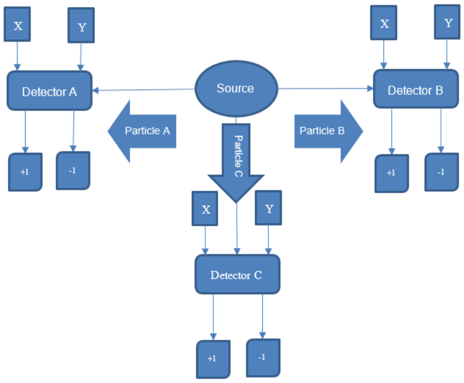


Figure 5: A schematic representation of the GHZ device and its three detectors

2) *Hidden Value Argument*

Table 4 shows the combined outcomes (outputs), according to the inputs (settings) for each particle once they collapse on each of their detectors if a hidden values argument is used.

Table 4: Measurement for the combined value of possible outcomes to succeed

Setting (r) in detector A	Setting (s) in detector B	Setting (t) in detector C	Condition to succeed	Measurement for the combined value of possible outcomes to succeed $m_{abc} = (a \times b \times c)$
$r = \mathrm{X}$	$s = \mathrm{X}$	$t = \mathrm{X}$	ODD number of +1's as output	$+1 \times +1 \times +1 = +1$ $+1 \times -1 \times -1 = +1$ $-1 \times +1 \times -1 = +1$ $-1 \times -1 \times +1 = +1$
$r = \mathrm{X}$	$s = \mathrm{Y}$	$t = \mathrm{Y}$	EVEN number of +1's as output	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$
$r = \mathrm{Y}$	$s = \mathrm{X}$	$t = \mathrm{Y}$	EVEN number of +1's as output	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$
$r = \mathrm{Y}$	$s = \mathrm{Y}$	$t = \mathrm{X}$	EVEN number of +1's as output	$+1 \times +1 \times -1 = -1$ $+1 \times -1 \times +1 = -1$ $-1 \times +1 \times +1 = -1$ $-1 \times -1 \times -1 = -1$

The detectors could have settings X or Y (polarized filters in x or y-direction).

The individual values of measurement $(a, b\ or\ c)$ could be either +1 (photon passes through the polarizer) or -1 (photon is blocked).

The combined value of the outcome m_{abc} is a multiplication of their values $a, b\ and\ c$.

In summary, although there are 8 possible arrangements $\{XXX; XYY; YXY; YYX; YXX; XYX; XXY; YYY\}$, there are only 4 arrangements of settings with relevant useful information in the context under study $\{XXX; XYY; YXY; YYX\}$.

Choosing the value for X in detector A, B and C of +1, it is easy to conclude that the combined measurement is +1.

This means that, to continue to have a successful simulation, the output of detectors B and C, knowing that Y is the input for both, should have opposite values of output (one should have +1 and the other should have value -1), because the combined value should be -1 ($m_{abc} = a \times b \times c = -1$). It is possible to make again an arbitrary choice (because there are two possible choices) of having an output of -1 for detector B, if Y is the input and +1 for detector C, if Y is input.

To continue to have successful simulation, the value output value in detector A, knowing that the input is Y should be -1, otherwise, it's impossible to get $m_{abc} = a \times b \times c = -1$, because in earlier tables were already defined that if detector B has X as input then output is +1 and if detector C has Y as input then output is +1.

Finally, with earlier choices we have all hidden values defined:

- If Detector A has X as input, then the output is +1;
- If Detector A has Y as input, then the output is -1;
- If Detector B has X as input, then the output is +1;
- If Detector B has Y as input, then the output is +1;
- If Detector C has X as input, then the output is +1;
- If Detector C has Y as input, then the output is -1.

And with these hidden values defined it's impossible to have a successful simulation for the arrangement $\{YYX\}$ because the combined value $m_{abc} = a \times b \times c = +1$, instead of -1.

Hence, it's only possible to win $\frac{3}{4}$ of times using these hidden values. If the same exercise is done for all hidden values and arrangements the conclusion will always be the same: it's impossible to always win the game using a hidden value approach.

3) *Quantum Mechanics (QM) Argument*

In the previous subchapter, it was shown that it's impossible to always win the game using the hidden value approach. In this subchapter, we will see if it's possible to always win the game with the quantum mechanics approach.

Each particle has its properties. So particle A is represented with $|\,\psi\,\rangle_{\boldsymbol{A}}$, Particle B with$|\,\psi\,\rangle_{\boldsymbol{B}}$ and Particle C with$|\,\psi\,\rangle_{\boldsymbol{C}}$

$$|\,\psi\,\rangle_{\boldsymbol{A}} = \alpha_A\,|\,0\,\rangle_{\boldsymbol{A}} + \beta_A\,|\,1\,\rangle_{A}, \qquad \alpha, \beta\ \in \mathbb{C} \qquad (26)$$

$$|\,\psi\,\rangle_{\boldsymbol{B}} = \alpha_B\,|\,0\,\rangle_{\boldsymbol{B}} + \beta_B\,|\,1\,\rangle_{B}, \qquad \alpha, \beta\ \in \mathbb{C} \qquad (27)$$

$$|\,\psi\,\rangle_{\boldsymbol{C}} = \alpha_C\,|\,0\,\rangle_{\boldsymbol{C}} + \beta_C\,|\,1\,\rangle_{C}, \qquad \alpha, \beta\ \in \mathbb{C} \qquad (28)$$

But when particles are entangled states are inseparable, hence cannot be studied as separate states.

This means that the result of entangled photons are always equal when they collapse on their respective detector, as a result, they flash the same output with the same setting.

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\,[|000\rangle_{ABC} + |111\rangle_{ABC}\,] \qquad (29)$$

Not considering the entanglement factor, each measurement could be done in the x-axis (X) or y-axis (Y), meaning that in the original state a linear transformation is applied, in order the get measurement in the desired axis.

To get a measurement in the x-axis, the Pauli matrix σ_x should be applied to the original state:

$$(\sigma_x)|0\rangle = \ |1\rangle \qquad (30)$$

$$(\sigma_x)|1\rangle = \ |1\rangle \qquad (31)$$

To get a measurement in the y-axis, the Pauli matrix σ_y is applied should be applied to the original state:

$$(\sigma_y)|0\rangle = i|1\rangle \qquad (32)$$

$$(\sigma_y)|1\rangle = -i|0\rangle \qquad (33)$$

There are 4 arrangements of settings with useful information in the context that is being studied $\{XXX; XYY; YXY; YYX\}$, it is also possible to have 4 combined measurements.

The measurements for each arrangement to the state $|\Psi\rangle_{ABC}$ are given by the eigenvalues m_{abc} of the following transformations:

$$(\sigma_x \otimes \sigma_x \otimes \sigma_x)|\Psi\rangle_{ABC} = +|\Psi\rangle_{ABC}, \qquad m_{abc} = +1 \qquad (34)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \qquad m_{abc} = -1 \qquad (35)$$

$$(\sigma_y \otimes \sigma_x \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \qquad m_{abc} = -1 \qquad (36)$$

$$(\sigma_x \otimes \sigma_y \otimes \sigma_y)|\Psi\rangle_{ABC} = -|\Psi\rangle_{ABC}, \qquad m_{abc} = -1 \qquad (37)$$

In conclusion, we have a probability of scoring equal to 100% using quantum mechanics.

III. Quantum Computation

A. Qubit

Qubit (also known as Quantum Bit) is the fundamental unit of quantum computation. It is essential to make operations and to create algorithms to solve logic problems. In classical computation, the essential units are called bits and have values of 0 and 1. Qubits are usually represented with kets $|0\rangle$ and $|1\rangle$. In mathematical terms the units could be represented as vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{38}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{39}$$

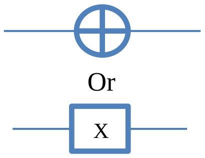
In classical computation, the unit should be in one of the states 0 or 1, however, quantum computation allows the superposition between the two states $|0\rangle$ and $|1\rangle$.
So one qubit could be represented by ket $|\,\psi\,\rangle$

$$|\,\psi\,\rangle = \alpha\,|\,0\,\rangle + \beta\,|\,1\,\rangle, \qquad \alpha, \beta\ \in \mathbb{C} \tag{40}$$

Where α and β are the amplitudes with probabilities of $|\alpha|^2$,$|\beta|^2$ and $|\alpha|^2 + \ |\beta|^2 = 1$

B. Quantum Gates Representation

Quantum gates represent the transformation of Qubit from one state to another. They are necessary to make logical operations. There are 2 types of quantum gates: single-qubit gates and multiple qubit gates. With single-qubit gates, there is a logical transformation of the unit that performs the negation of the initial state. This Unitary and Hermitian gate is called NOT gate (also known as Pauli-X Gate) and could be represented with the following circuit diagram and as Pauli X matrix.



$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

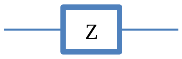
Figure 6: Circuit and matrix representation of NOT gate (Pauli-X)

Considering that the Pauli X gate represents the rotation around the x-axis in the Bloch sphere, it is possible to have rotation around the other two axes (Y or Z). Having said this, Pauli-Y Gate is represented by:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Figure 7: Circuit and matrix representation of Pauli-Y Gate

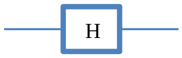
Pauli-Z Gate is represented by:



$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Figure 8: Circuit and matrix representation of Pauli-Z Gate

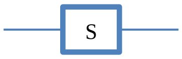
Besides Pauli gates, there are several other one-bit gates. The Hadamard gate is very important because it can introduce a superposition into a well-defined input state $|0\rangle$ or $|1\rangle$.
The Hadamard gate is represented by:



$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Figure 9: Circuit and matrix representation of Hadamard Gate

Another possible gate is Phase Gate, represented in Figure 10:



$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

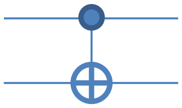
Figure 10: Circuit and matrix representation of Phase Gate

$\pi/8$ gate (also denoted as T Gate) is represented by:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

Figure 11: Circuit and matrix representation of T Gate

It is also possible to make operations with multiple qubits. Quantum computation requires that all operations and gates are reversible, meaning that all outputs should have a unique input.
The gate to make multiple bit operations is called the CNOT gate and it is represented as it follows (two-qubit representation):



$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 12: Circuit and matrix representation of CNOT Gate

C. Quantum Parallelism

In the earlier chapter, it was seen that quantum gates are essential to make logical operations. Although one gate is important, sometimes complex problems cannot be solved using a single gate, thus it's necessary to have a quantum circuit with several gates. One big advantage used in quantum circuits is quantum parallelism. Quantum parallelism allows having several values of output simultaneously in a single run. Bellow, it will be shown mathematically how that is possible.

Considering a binary function f and an oracle U_f making the following transformation:

$$U_f: |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle \qquad (41)$$

An oracle is usually used in computation to represent a black box containing a circuit. To explain the problem and the solution it's not necessary to define the content of the black box, it's only important to know the behavior. Being said that, the circuit representation of (41) is:

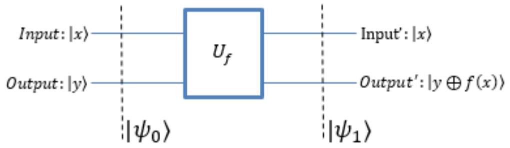


Figure 13: Oracle U_f transforming $|x, y\rangle$ into $|x, y \oplus f(x)\rangle$

If $|x\rangle$ is equal to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ (state in sobreposition) and $|y\rangle$ is equal to$|0\rangle$, then $|\psi_1\rangle$ is:

$$|\psi_1\rangle = U_f|\psi_0\rangle \qquad (42)$$

$$|\psi_1\rangle = |x, y \oplus f(x)\rangle \qquad (43)$$

$$|\psi_1\rangle = \frac{(|0, f(0)\rangle + |1, f(1)\rangle)}{\sqrt{2}} \qquad (44)$$

And this concludes that state $|\psi_1\rangle$ contains information about $f(0)$ and $f(1)$, simultaneously, in a single run.

IV. Shor's Algorithm

In this chapter, the goal is to find a period of a function using a quantum computation algorithm and give it a practical utility. The period of a function f(x) is a repetition of values at regular intervals of multiples k of x. Finding the period (of a periodic) function is the key to factoring products of large prime numbers. This is not an easy task, and that is why the most common security protocol to encrypt information nowadays RSA (Rivest–Shamir–Adleman) protocol exploits this difficulty. Shor's factoring algorithm will make breaking RSA protocol easier. In the next subchapters, it will be explained how.

A. RSA Protocol

Before trying to break the RSA protocol, it is important to understand how it works.

RSA protocol is a secure encryption protocol that encrypts a message in a way that it's almost impossible to decrypt by knowing only the encrypted message and the encryption rule (key). Four steps are involved:

1. Key Generation;
2. Key Distribution;
3. Message encryption;
4. Message decryption;

In the key generation phase two keys (K_s and K_p) are generated

K_s is the secret key (also known as private key) with components (d and M).

K_p is the public key with components (e and M).

To generate the keys the following rules should be followed:

Choose two prime numbers (meaning that the numbers should have only 2 factors: 1 and themselves): p and q

Compute $M = pq$ (M equals to p times q)

Choose e in the way that $1 < e < \phi(M)$, where $\phi(M) = (p-1)(q-1)$

Being $\phi(M)$ the Euler's totient function (a function that gives the number of integers that are coprime to M) with the following property:

$\phi(p) = (p-1)$, a specific case of $\phi(M) = \prod_{M|p} M\left(1 - \frac{1}{p}\right)$, for prime $p > 1$

$\phi(q) = (q-1)$, a specific case of $\phi(M) = \prod_{M|q} M\left(1 - \frac{1}{q}\right)$, for prime $q > 1$

$$\phi(M) = \phi(p)\,\phi(q) = (p-1)(q-1)$$

Moreover the greatest common divisor between e and $\phi(M)$ (the largest positive integer that divides each of the integers) are equal to 1: $\gcd(e, \phi(M)) = 1$

Compute d in the way that $1 < d < \phi(M)$, where

$$\phi(M) = (p-1)(q-1)$$

And $\underbrace{ed}_{a} \equiv \underbrace{1}_{b} \left(mod\left(\underbrace{\phi(M)}_{S}\right)\right)$

These two integers (a and b) are said to be congruent S, if $S > 1 \in \mathbb{Z}$ is a divisor of their difference (a− b = kS): The congruence relation could be written as a = kS + b

The encryption process is described by the below example:

Alice sends a message to Bob

Alice receives from Bob the public key $K_p \rightarrow (M, e)$

Alice transforms the message (Text) into an integer (using for example the ASCII Code) T

Alice sends to Bob ciphertext C:

$$C \equiv T^e\left(mod(M)\right)$$

Bob receives the message and understands the content

Bob receives the ciphertext C

$$C \equiv T^e\left(mod(M)\right)$$

Having the secret key $K_s \rightarrow (M, d)$, bob applies d on C

$C^d \equiv \left(T^e\left(mod(M)\right)\right)^d$

Since $ed \equiv 1\left(mod\left(\phi(M)\right)\right)$, the result becomes:

$$C^d \equiv T^{ed}\left(mod(M)\right)$$

$$C^d \equiv T^{ed}\left(mod(M)\right) = T^{k\phi(M)+1}\left(mod(M)\right)$$

$$C^d \equiv T^{\phi(M)^k}.T^1\left(mod\,(M)\right)$$

Applying Euler's Theorem the result becomes

$$C^d \equiv T^{M-1^k}.T^1\left(mod(M)\right)$$

Applying Fermat's Little Theorem the result becomes

$$C^d \equiv 1^k.T^1\left(mod(M)\right) = T$$

Convert T to letters (using for example ASCII Code)

B. Breaking RSA Protocol

One of the practical utilities that the Shor algorithm has is breaking the RSA protocol. The Shor Algorithm has several steps that can be computed by classical computers. One of the steps should be performed by a quantum computer. The step performed by quantum computation is finding the period of modular arithmetic.

Steps to break RSA protocol

1) Firstly, to find factors (p and q) of the number M (seen in the earlier subchapter), it's necessary to find a coprime number a with M (meaning a don't share any common divisor with M).

   Choose an a, with the condition:

$$\gcd(a, M) = 1 \tag{45}$$

2) Using quantum computation find the smallest r of the function that makes the statement $a^r mod(M) \equiv 1\, mod(M)$ true.

Being r a period representation of the modular arithmetic of M, r can be repeated k times. This means that the function $f(x)$ is equal to $f(x + kr)$

$$\begin{aligned} f(x) = f(x+kr) \equiv \mathrm{a}^x \left(mod(M)\right) \\ = \mathrm{a}^{x+kr} \left(mod(M)\right), \\ k \; and \; r \in \mathbb{N} \end{aligned} \tag{46}$$

3) Having calculated the value of r, it's necessary to validate if r is even or if it is odd.
   a) If the value of r is odd:
      i) It's necessary to choose a new value of a and run step 1) again.
   b) If the value of r is even:
      i) It's necessary to calculate b:

$$b \equiv a^{\frac{r}{2}} \left(mod(M)\right) \tag{47}$$

(1) If $b + 1 \not\equiv 0 \left(mod(M)\right)$ then

$$\{p, q\} = \{\gcd(b + 1, M), \gcd(b - 1, M)\} \tag{48}$$

(2) Else It's necessary to choose a new value of a and do step 1) again.

Having p and q, it's possible to find e and d using the steps of the subchapter containing steps to compute RSA protocol.

1) Quantum circuit to find period r

To find period r using quantum computation, it's necessary to define the quantum circuit.

And the circuit is defined in Figure 14.

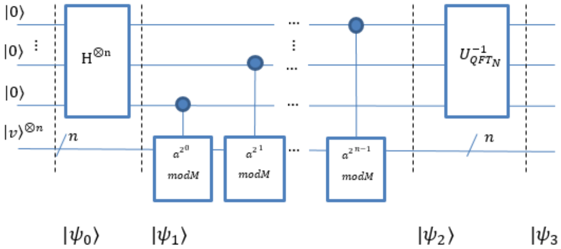


Figure 14: Shor circuit to find period r

Now it's possible to use quantum phase estimation on the unitary operator:

$$\mathrm{U}|y\rangle \equiv |ay \; mod \; M\rangle \tag{49}$$

It's possible to find the period r (first integer different than zero that turns $a^r \; mod \; M = 1$) from a unitary Matrix U with eigenvector $|u\rangle$ and eigenvalue λ:

$$\mathrm{U}|u\rangle = \lambda|u\rangle \tag{50}$$

Where λ could be represented as $\lambda = e^{2\pi i\theta}$ as seen QPE subchapter (because this problem is in the fact a QPE disguised)

$$\mathrm{U}|u\rangle = e^{2\pi i\theta}|u\rangle \tag{51}$$

Where the eigenvector is:

$$|u\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2\pi i k}{r}}|a^k \; mod \; M\rangle \tag{52}$$

And the result is calculated as follows:

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |v\rangle^{\otimes n} \tag{53}$$

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + |1\rangle)^{\otimes n}] \otimes |v\rangle^{\otimes n} \tag{54}$$

$$\begin{aligned} |\psi_2\rangle = \left(\frac{1}{\sqrt{2}}\right)^n [(|0\rangle + U^{2n-1}|1\rangle) \otimes \dots \\ \otimes \left(|0\rangle + U^{2^0}|1\rangle\right)] \otimes |v\rangle \end{aligned} \tag{55}$$

$$\begin{aligned} |\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}}\right)\Big[(|0\rangle + e^{2\pi i\theta^{2n-1}}|1\rangle) \otimes \dots \otimes (|0\rangle \\ + e^{2\pi i\theta^{2^0}}|1\rangle)\Big] \otimes |v\rangle \end{aligned} \tag{56}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi i k\theta}|k\rangle \otimes |v\rangle \tag{57}$$

The inverse QFT is given by:

$$U_{QFT_N}^{-1} = \left[\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\sum_{j=0}^{2^n-1} e^{\frac{2\pi i k j}{2^n}}|k\rangle\right]^{-1} \tag{58}$$

And the relation between phase θ and $k \; is \; given \; by$ is:

$$\theta = \frac{k}{2^n} \tag{59}$$

$$2^n\theta = k \tag{60}$$

And r is given by

$$k = 2^n . \frac{s}{r} \quad (61)$$

With s being a random integer between 0 and $r - 1$. Concluding the result becomes:

$$|\psi_3\rangle = |2^n . \frac{s}{r}\rangle \otimes |v\rangle \quad (62)$$

V. Conclusion

As stated in the introduction, the computer field started with Alan Turing in 1936 [2], and the study of the quantum computing field started in 1982 with Richard Feynman [6]. In the beginning, it was a theoretical study. Then, theoretical concepts started to become more known and more solid. Concepts such as Shor's Algorithm (originally designed to solve the problem of large number factorization) appeared, exposing some vulnerabilities of encryption codes such as RSA encryption code. The latest version is the RSA-2048 (which consists of a number with 617 decimal digits, equivalent to 2048 bits, which are commonly used to exchange encrypted messages between two parties).

In 2016, a real five-qubit computer was introduced to the world by IBM [14]. Although this was 5 years ago, today it is still not possible to have a fully functional computer with more than 200 qubits.

Building a quantum computer is only useful if it can solve problems that no classical computer can solve in a feasible amount of time (such as factoring products of large prime numbers). When a quantum computer can do this it means that Quantum Supremacy was reached [15].

The main reason for not reaching yet this era is Quantum Decoherence. Quantum Decoherence is the opposite of coherence, meaning that the result could be faulty, being impossible to know a result without errors and that affects the output result. In classical computation, the problem is solved mainly by adding redundancy. In quantum computation, the same is not possible because of the no-cloning theorem, which affirms that it is impossible to make a copy of a unitary state (qubit state) out of another unitary state [16]. There are two ways to solve this issue: by creating a quantum computer with more stable qubits or by improving quantum error correction techniques. Both solutions are complicated to implement, but there is still hope and every year we see small improvements that allow this field to grow.

According to the latest state of art Google's Craig Gidney and KTH's Martin Ekera quantum journal paper, it will be necessary to build a quantum computer with 20 million qubits to break the RSA-2048 encryption code using an improved version of Shor's algorithm [17].

Although there seems to be a long way to go, history has taught us that change will happen and perhaps, sooner than we expect.

VI. References

[1] T. Corman, C. Leiserson, R. Rivest and C. Stein, Introduction to Algorithms, 2nd ed., McGraw-Hill, 2002.

[2] A. M. Turing, "On computable numbers, with an application to the Entscheidungsproblem," Proceedings of the London Mathematical Society, vol. 42, pp. 230-265, 1937.

[3] J. v. Neumann, "First Draft of a Report on the EDVAC," IEEE Annals of the History of Computing, vol. 15, pp. 27-75, 1993.

[4] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[5] G. E. Moore, "Cramming more components onto integrated circuits," Electronics, vol. 38, 1965.

[6] R. P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, pp. 467-488, 1982.

[7] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proceedings of the Royal Society of London, pp. 97-117, 1985.

[8] N. D. Mermin, "BOOJUMS ALL THE WAY THROUGH: Communicating Science in a Prosaic Age," New York, Cambridge University Press, 1990.

[9] A. Einstein, B. Podolsky and N. Rosen , "Can quantum-mechanical description of physical reality be considered complete?," Physical Review, p. 777–780, 1935.

[10] J. S. Bell, "On the Einstein Podolsky Rosen Paradox," Physics, Physique, Fizika, p. 777–780, 1964.

[11] A. Aspect, P. Grangier and G. Roger, "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedanken experiment: A New Violation of Bell's Inequalities," Phys. Rev. Let, vol. 49, pp. 91-94, 1982.

[12] S. Popescu and D. Rohrlich , "Quantum Nonlocality as an Axiom," Foundations of Physics, vol. 24, p. 379, 1994.

[13] D. Greenberger, M. Horne, A. Shimony and A. Zeilinger, "Bell's theorem without inequalities," American Journal of Physics, no. 58 (12), pp. 1131-1143, 1990.

[14] C. Bernhardt, Quantum Computing for Everyone, The MIT Press, 2019, p. 183.

[15] J. Preskill, "Quantum computing and the entanglement frontier," in The Theory of the Quantum Worl, Brussels, 2011.

[16] W. Wootters and W. Zurek, "A Single Quantum Cannot be Cloned," Nature, vol. 299, pp. 802-803, 1982.

[17] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," Quantum, vol. 5, p. 433, 2021.