

Quantum Fourier transform of the Prime state

Author: Eduard Ribas Fernández
*Facultat de Física i Facultat de Matemàtiques,
Universitat de Barcelona, Barcelona, Spain.*

Advisor: Dr. José Ignacio Latorre Sentís
*Departament d'Estructura i Constituents de la Matèria,
Facultat de Física, Universitat de Barcelona, Barcelona, Spain.*

Quantum Computation is a growing and important field in applied physics research, so further theoretical foundations are continuously requested. In this regard, some mathematical algorithms have already been proposed. For instance, creating a quantum state representing the superposition of all prime number less than a value N has been shown to be efficient, and also applying the Quantum Fourier transform to it. This paper discusses the result of doing this operation and shows that some deep mathematical properties of prime numbers, such the *Prime Counting function* or biases in primes distribution, like the *Chebyshev bias*, are easily accessible via a systematic statistical approach.

I. INTRODUCTION

Quantum computers are rapidly becoming a reality, thanks to the investment and research carried out by scientific institutions, companies and governments. Two gigantic technology companies are taking part of this quantum race: *Google Inc.*[®] and *IBM*[®]. The former collaborates with two pioneering teams: *D-Wave Systems*, which have its 1152-qubit D-Wave 2X quantum annealer computer [1]; and Martinis Group, who promises a 100-qubit computer in few years [2]. The latter has recently made public his cloud-based quantum computing platform, the *IBM Quantum Experience* [3, 4], a 5-qubit quantum computer.

Quantum computers will allow for developing faster and more secure algorithms and communications. One application of these powerful algorithms would be solving mathematical problems, testing or rejecting hypothesis and conjectures, but there is still work to be done.

In this paper we discuss a systematic application of the *Quantum Fourier transform* to a quantum *Prime state* (superposition of prime numbers), whose results give statistical access to arithmetic properties of prime numbers and their distribution, like the *Prime Counting Function*, the *Modular Prime Counting Functions* and the *Chebyshev bias* [5–8].

II. MATHEMATICAL DEFINITIONS

Let \mathbb{P}_N be the set of prime numbers less than N ,

$$\mathbb{P}_N := \{p \text{ prime}, p < N\}. \quad (1)$$

Then, the *Prime Counting Function* $\pi(N)$ gives the number of primes less than N , i.e.,

$$\pi(N) := \sum_{p \in \mathbb{P}_N} 1 = \#\mathbb{P}_N. \quad (2)$$

The *Modular Prime Counting Functions* $\pi_{a,b}(N)$, when $\gcd(a,b) = 1$, is defined similarly:

$$\begin{aligned} \pi_{a,b}(N) &:= \sum_{\substack{p \in \mathbb{P}_N \\ p \equiv b \pmod{a}}} 1 \\ &= \#\{p \in \mathbb{P}_N, p \equiv b \pmod{a}\}. \end{aligned} \quad (3)$$

Thus, given $a \in \mathbb{N}$, it is deduced that

$$\pi(N) = \sum_{b=0}^{a-1} \pi_{a,b}(N) \quad (4)$$

In particular, $\pi_{4,1}(N)$ and $\pi_{4,3}(N)$ are *equinumerous*, which means that

$$\pi_{4,1}(N) \sim \pi_{4,3}(N),$$

but Chebyshev noted, and Hardy and Littlewood later proved that

$$\Delta_{4;3,1}(N) := \pi_{4,3}(N) - \pi_{4,1}(N) \quad (5)$$

changes sign infinitely often. This effect is called the *Prime Quadratic Effect*, and $\Delta(N) := \Delta_{4;3,1}(N)$ is known as *Chebyshev Bias* [8, 9].

III. PRIME STATE

We can define the *Prime state* of n -qubits as the quantum state superposition of every prime number less than $N = 2^n$, i.e.,

$$|\mathbb{P}_N\rangle := \frac{1}{\sqrt{\pi(N)}} \sum_{p \in \mathbb{P}_N} |p\rangle. \quad (6)$$

Each prime number can be expressed in its binary form,

$$p = p_0 \cdot 2^0 + p_1 \cdot 2^1 + \dots + p_{n-1} \cdot 2^{n-1},$$

so its quantum state can be represented in terms of the n -qubit as follows:

$$|p\rangle = |p_{n-1}, \dots, p_1, p_0\rangle.$$

Latorre and Sierra [10, 11] propose a computational efficient way to prepare this Prime state, which consists in using a primality test (like the Miller-Rabin's one, or even the AKS, which is deterministic, efficient and unconditioned to the validity of the Riemann Hypothesis) as an oracle in Grover's search algorithm in order to find the $\pi(2^n)$ primes within the numbers less than 2^n .

IV. QUANTUM FOURIER TRANSFORM OF THE PRIME STATE

The *Quantum Fourier transform* (QFT) is a generalization of the classic *Discrete Fourier transform*. It efficiently gives access to hidden information of the wave function of the state [12, 13].

If we consider the following state in the computational basis [14],

$$|\psi\rangle = \sum_{j=0}^{N-1} f(j)|j\rangle, \quad (7)$$

its QFT is

$$|\tilde{\psi}\rangle = U_{QFT}|\psi\rangle = \sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle, \quad (8)$$

where

$$\tilde{f}(k) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i}{N}jk} f(j). \quad (9)$$

If we want to apply the QFT to the Prime state, it is useful to write (6) as

$$\begin{aligned} |\mathbb{P}_N\rangle &= \frac{1}{\sqrt{\pi(N)}} \sum_{p \in \mathbb{P}_N} |p\rangle \\ &= \sum_{j=0}^{N-1} f(j)|j\rangle \end{aligned} \quad (10)$$

where

$$f(j) := \begin{cases} \frac{1}{\sqrt{\pi(N)}} & , \text{ if } j \in \mathbb{P}_N \\ 0 & , \text{ otherwise} \end{cases} \quad (11)$$

Then, applying (8) to (10):

$$\begin{aligned} |\tilde{\mathbb{P}}_N\rangle &= U_{QFT}|\mathbb{P}_N\rangle = \sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle \\ &= \frac{1}{\sqrt{N\pi(N)}} \sum_{k=0}^{N-1} \left(\sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N}kp} \right) |k\rangle. \end{aligned} \quad (12)$$

V. PEAKS AND BIASES

The state (12) is a superposition of the states $|0\rangle, \dots, |N-1\rangle$, so the probability of measuring one of them, $|k\rangle$, is given by the square of its coefficient:

$$Prob(k) = \frac{1}{N\pi(N)} \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N}kp} \right|^2. \quad (13)$$

For certain values of the phase k , the terms of the sum overlap in a way that this probability has a remarkable meaning (numerical simulations like the one shown in Fig.(1) give an idea of which values may be interesting). We will discuss some of these cases but, to make it more clear, we will omit the normalization factor of the probability peaks:

$$P(k) = \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N}kp} \right|^2. \quad (14)$$

A. Symmetry

The first fact we can observe from the probability (14) is that it is symmetric with respect to the value $k = \frac{N}{2}$, meaning that the registers $|k\rangle$ and $|N-k\rangle$ have the same probability of being measured:

$$\begin{aligned} P(N-k) &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N}(N-k)p} \right|^2 = \left| \sum_{p \in \mathbb{P}_N} e^{-\frac{2\pi i}{N}kp} \right|^2 \\ &= \left| \sum_{p \in \mathbb{P}_N} \cos\left(\frac{2\pi kp}{N}\right) - i \sum_{p \in \mathbb{P}_N} \sin\left(\frac{2\pi kp}{N}\right) \right|^2 \\ &= \left| \sum_{p \in \mathbb{P}_N} \cos\left(\frac{2\pi kp}{N}\right) + i \sum_{p \in \mathbb{P}_N} \sin\left(\frac{2\pi kp}{N}\right) \right|^2 \\ &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N}kp} \right|^2 \\ &= P(k) \end{aligned} \quad (15)$$

Consequently, the following discussion about peaks can be extended to their symmetrical values.

B. Prime Counting function

Firstly, we can easily relate the $k = 0$ peak with the value of the Prime Counting function, $\pi(N)$:

$$P(0) = \left| \sum_{p \in \mathbb{P}_N} e^0 \right|^2 = \left| \sum_{p \in \mathbb{P}_N} 1 \right|^2 = \pi(N)^2. \quad (16)$$

Another relation is obtained when $k = \frac{N}{2}$. Using (3) and (4) with $a = 2$,

$$\pi_{2,0}(N) = \#\{p \in \mathbb{P}_N, p \equiv 0 \pmod{2}\} = \#\{2\} = 1,$$

so

$$\pi_{2,1}(N) = \#\{p \in \mathbb{P}_N, p \equiv 1 \pmod{2}\} = \pi(N) - 1,$$

and then:

$$\begin{aligned} P\left(\frac{N}{2}\right) &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{N} \frac{N}{2} p} \right|^2 = \left| \sum_{p \in \mathbb{P}_N} e^{p\pi i} \right|^2 \\ &= \left| \sum_{\substack{p \in \mathbb{P}_N \\ p \equiv 0 \pmod{2}}} e^{p\pi i} + \sum_{\substack{p \in \mathbb{P}_N \\ p \equiv 1 \pmod{2}}} e^{p\pi i} \right|^2 \\ &= |\pi_{2,0}(N)e^0 + \pi_{2,1}(N)e^{\pi i}|^2 \\ &= |1 - (\pi(N) - 1)|^2 \\ &= \pi(N)^2 - 4\pi(N) + 4. \end{aligned} \quad (17)$$

C. Chebyshev bias: $\Delta(N) = \Delta_{4;3,1}(N)$

Similarly, the Chebyshev bias can be found in the peak $k = \frac{N}{4}$. In this case, we consider the following decomposition of the Prime Counting function

$$\pi(N) = \pi_{4,0}(N) + \pi_{4,1}(N) + \pi_{4,2}(N) + \pi_{4,3}(N)$$

but $\pi_{4,0}(N) = 0$ and $\pi_{4,2}(N) = \#\{2\} = 1$. Then:

$$\begin{aligned} P\left(\frac{N}{4}\right) &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{\pi i}{2} p} \right|^2 \\ &= \left| \pi_{4,1}(N)e^{\frac{\pi i}{2}} + \pi_{4,2}(N)e^{\pi i} + \pi_{4,3}(N)e^{\frac{3\pi i}{2}} \right|^2 \\ &= |1 + i(\pi_{4,3}(N) - \pi_{4,1}(N))|^2 \\ &= |1 + i\Delta_{4;3,1}(N)|^2 = 1 + \Delta(N)^2. \end{aligned} \quad (18)$$

D. Other biases: $\Delta_{3;2,1}(N)$, $\Delta_{6;5,1}(N)$

We can generalize the definition of the Chebyshev bias (5) to

$$\Delta_{a;b,b'}(N) := \pi_{a,b}(N) - \pi_{a,b'}(N) \quad (19)$$

In particular, $\pi_{3,1}(N)$ and $\pi_{3,2}(N)$ are also equinumerous [8], so the bias

$$\Delta_{3;2,1}(N) := \pi_{3,2}(N) - \pi_{3,1}(N)$$

is another interesting value. We can obtain it by considering $k = \frac{N}{3}$, an using that

$$\pi(N) = \pi_{3,0}(N) + \pi_{3,1}(N) + \pi_{3,2}(N)$$

with $\pi_{3,0}(N) = \#\{3\} = 1$, so $\pi_{3,1}(N) + \pi_{3,2}(N) = \pi(N) - 1$:

$$\begin{aligned} P\left(\frac{N}{3}\right) &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{2\pi i}{3} p} \right|^2 \\ &= \left| 1 + \pi_{3,1}(N)e^{\frac{2\pi i}{3}} - \pi_{3,2}(N)e^{\frac{4\pi i}{3}} \right|^2 \\ &= \left| 1 + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\pi_{3,1}(N) + \left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\pi_{3,2}(N) \right|^2 \\ &= 1 + \frac{1}{4}(\pi_{3,1}(N) + \pi_{3,2}(N))^2 - \pi_{3,1}(N) - \pi_{3,2}(N) + \frac{3}{4}(\pi_{3,1}(N) - \pi_{3,2}(N))^2 \\ &= \Delta_{3;2,1}(N)^2 + \pi_{3,1}(N)\pi_{3,2}(N) - \pi(N) + 2. \end{aligned} \quad (20)$$

The last situation we are going to consider is $k = \frac{N}{6}$. The Prime Counting function can be split in six terms:

$$\begin{aligned} \pi(N) &= \pi_{6,0}(N) + \pi_{6,1}(N) + \pi_{6,2}(N) + \\ &\quad + \pi_{6,3}(N) + \pi_{6,4}(N) + \pi_{6,5}(N), \end{aligned}$$

but $\pi_{6,0}(N) = 0$, $\pi_{6,2}(N) = \#\{2\} = 1$ and $\pi_{6,3}(N) = \#\{3\} = 1$. Considering the bias

$$\Delta_{6;5,1}(N) := \pi_{6,5}(N) - \pi_{6,1}(N),$$

we compute the peak:

$$\begin{aligned} P\left(\frac{N}{6}\right) &= \left| \sum_{p \in \mathbb{P}_N} e^{\frac{\pi i}{3} p} \right|^2 \\ &= \left| \pi_{6,1}(N) \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) + \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) - 1 + \pi_{6,5}(N) \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \right|^2 \\ &= \Delta_{6;5,1}(N)^2 + \pi_{6,1}(N)\pi_{6,5}(N) - 3\pi_{6,5}(N) + 3. \end{aligned} \quad (21)$$

We observe that equations (20) and (21) are very similar, so we can try to establish a relation between them. Indeed, first we need to see the relation between the Modular Prime Counting functions involved:

- A prime p is counted by $\pi_{3,1}(N)$ if there is $k \in \mathbb{Z}$ that $p = 3k + 1$, but because p is odd, k has to be even, so $k = 2k'$, and then $p = 6k' + 1$, which means that p is also counted by $\pi_{6,1}(N)$. Arguing inversely, it can be deduced that

$$\pi_{3,1}(N) = \pi_{6,1}(N). \quad (22)$$

- On the other hand, p is counted by $\pi_{3,2}(N)$ if $p = 3k+2$ with k odd, so $p = 3(2k'+1)+2 = 6k'+5$, which means p is counted by $\pi_{6,5}(N)$. 2 is the only prime number counted by $\pi_{3,2}(N)$ and not by $\pi_{6,5}(N)$, so we have that

$$\pi_{3,2}(N) = \pi_{6,5}(N) + 1. \quad (23)$$

Using (22) and (23) with equation (21),

$$\begin{aligned} P\left(\frac{N}{6}\right) &= \Delta_{6,5,1}(N)^2 + \pi_{6,1}(N)\pi_{6,5}(N) - 3\pi_{6,5}(N) + 3 \\ &= \Delta_{3,2,1}(N)^2 + 1 - 2(\pi_{3,2}(N) - \pi_{3,1}(N)) + \\ &\quad + (\pi_{3,2}(N) - 1)\pi_{3,1}(N) - 3(\pi_{3,2}(N) - 1) + 3 \\ &= P\left(\frac{N}{3}\right) - 4\pi_{3,2}(N) + 2\pi_{3,1}(N) + 6 \end{aligned} \quad (24)$$

which entails that the peaks $P\left(\frac{N}{6}\right)$ and $P\left(\frac{N}{3}\right)$, both dominated by the cross product of Modular Prime Counting functions, have the same order of magnitude.

Finally, we can discuss how these four peaks $\left\{\frac{N}{6}, \frac{N}{3}, \frac{2N}{3}, \frac{5N}{6}\right\}$ compare to $k = 0$. Given that

$$\Delta_{3,2,1}(N) = \pi_{3,2}(N) - \pi_{3,1}(N)$$

and

$$\pi(N) - 1 = \pi_{3,2}(N) + \pi_{3,1}(N),$$

the Modular Prime Counting functions can be expressed like

$$\begin{aligned} \pi_{3,2} &= \frac{(\pi(N) - 1) + \Delta_{3,2,1}(N)}{2} \\ \pi_{3,1} &= \frac{(\pi(N) - 1) - \Delta_{3,2,1}(N)}{2}, \end{aligned}$$

Using these expressions on equation (20), we obtain

$$P\left(\frac{N}{3}\right) = \frac{3}{4}\Delta_{3,2,1}(N)^2 + \frac{1}{4}\pi(N)^2 - \frac{3}{2}\pi(N) + \frac{9}{4}. \quad (25)$$

Then, the difference between $P(0)$ and the sum of this four peaks is

$$\begin{aligned} P(0) - P\left(\frac{N}{6}\right) - P\left(\frac{N}{3}\right) - P\left(\frac{2N}{3}\right) - P\left(\frac{5N}{6}\right) &= \\ &= \pi(N)^2 - 2P\left(\frac{N}{3}\right) - 2P\left(\frac{N}{6}\right) \\ &= \pi(N)^2 - 4P\left(\frac{N}{3}\right) + 8\pi_{3,2}(N) - 4\pi_{3,1} - 12 \\ &= 8\pi(N) - 3\Delta_{3,2,1}(N)^2 + 6\Delta_{3,2,1}(N) - 23. \end{aligned} \quad (26)$$

This shows that the sum of the four peaks counteract the quadratic dominance of the peak $P(0) = \pi(N)^2$. A more visual and numerical approach is presented in the next section.

VI. NUMERICAL SIMULATION

Numerical simulations of the QFT of the Prime state can be performed with a classical computer [15]. Even if these simulations are not computationally efficient, becoming longer exponentially, they give an idea of the goodness of this method.

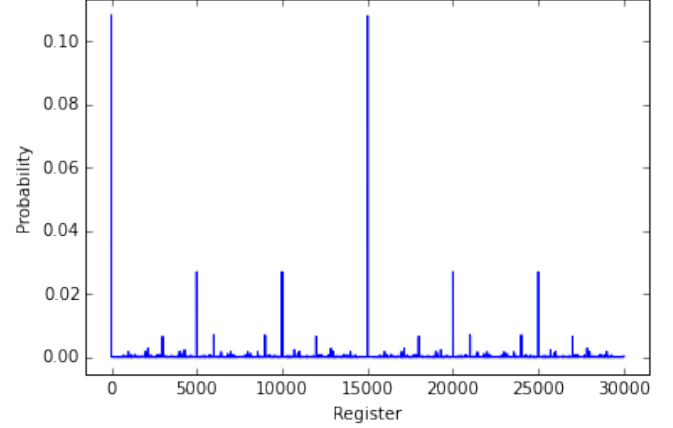


FIG. 1: Numerical simulation of the normalized Quantum Fourier transform of the Prime state for $N = 30000$. For each register $|k\rangle$, the plot shows its probability of being measured.

As an example, in Fig.(1) it is plotted the simulated normalized probability (13) of measuring each register $|k\rangle$ for a system with $N = 30000$. It can be seen the predominance of some of the previously studied peaks, but also the symmetry that we have discussed in section V A, (15). Peaks $k = 0$ and $k = \frac{N}{2}$ are much more bigger than the others, and about 4 times the size of peaks $k = \frac{N}{6}, \frac{N}{3}, \frac{2N}{3}, \frac{5N}{6}$, which all have the same order of magnitude

Register $ k\rangle$	Prob(k)	P(k)
0	0.108167...	10530025.0
$N/6$	0.026962...	2624763.0
$N/4$	$4.982023...e^{-6}$	485.0
$N/3$	0.026996...	2628073.0
$N/2$	0.108033...	10517049.0

TABLE I: Numerical values of the main peaks, normalized $[Prob(k)]$, and not $[P(k) = N\pi(N)Prob(k)]$, for $N = 30000$.

The precise values of these peaks are described more clearly in Table I. These values can be tested by using the formulas (16), (21), (18), (20) and (17) obtained previously in the discussion of section V, and the values of the prime functions in Table II:

- $P(0) = \pi(N)^2 = 3245^2 = 10530025$
- $P\left(\frac{N}{6}\right) = \Delta_{6,5,1}(N)^2 + \pi_{6,1}(N)\pi_{6,5}(N) - 3\pi_{6,5}(N) + 3 = 23^2 + 1610 \cdot 1633 - 4 \cdot 1633 + 3 = 2624763$

- $P\left(\frac{N}{4}\right) = 1 + \Delta(N)^2 = 1 + 22^2 = 485$
- $P\left(\frac{N}{3}\right) = \Delta_{3;2,1}(N)^2 + \pi_{3,1}(N)\pi_{3,2}(N) - \pi(N) + 2 = 24^2 + 1610 \cdot 1634 - 3245 + 2 = 2628073$
- $P\left(\frac{N}{2}\right) = \pi(N)^2 - 4\pi(N) + 4 = 3245^2 - 4 \cdot 3245 + 4 = 10517049$

Function	Value
N	30000
$\pi(N)$	3245
$\pi_{3,1}(N)$	1610
$\pi_{3,2}(N)$	1634
$\Delta_{3;2,1}(N)$	24
$\pi_{4,1}(N)$	1611
$\pi_{4,3}(N)$	1633
$\Delta_{4;3,1}(N)$	22
$\pi_{6,1}(N)$	1610
$\pi_{6,5}(N)$	1633
$\Delta_{6;5,1}(N)$	23

TABLE II: Prime Counting functions and biases for $N = 30000$.

VII. CONCLUSION

It has been shown that a Prime state can be efficiently created in a quantum computer, and that the Quantum

Fourier transform can be applied. Doing it repeatedly and measuring the final state, the peaks of the probability distribution obtained give a statistical approximation of some properties of prime numbers. For instance, some of these peaks are directly related to the Prime Counting function, the Chebyshev bias or the Modular Prime Counting Function.

In the near future, with powerful quantum computers, this method could be implemented and would allow for testing their performance. Moreover, in case of being further developed, this method could be used to study the behavior of prime numbers properties for larger values, and even testing or rejecting hypothesis.

Acknowledgement

I would like to express my gratitude to Dr. José Ignacio Latorre, whose advice and assistance have been essential for achieving this work. I am also grateful to Dr. Pilar Bayer, whose suggestions about prime numbers where enriching.

Finally, I would like to thank my family and friends for the support tendered all these years.

-
- [1] D-Wave Systems. D-Wave 2X, 2015. URL <http://www.dwavesys.com/d-wave-two-system>.
 - [2] University of California Santa Barbara. Martinis Group. URL <http://web.physics.ucsb.edu/~martinisgroup/>.
 - [3] IBM. IBM Quantum Experience, 2016. URL <http://www.research.ibm.com/quantum/>.
 - [4] D. Alsina and J. I. Latorre. Experimental test of Mermin inequalities on a 5-qubit quantum computer. 2016. URL <http://arxiv.org/abs/1605.04220>.
 - [5] B. Fine and G. Rosenberger. *Number theory - An introduction via the distribution of primes*. Birkhäuser Boston, Boston, MA, 2007.
 - [6] A. Travesa i Grau. *Aritmètica*. Edicions Universitat de Barcelona, Barcelona, 1998.
 - [7] H. Iwaniec and E. Kowalski. *Analytic number theory*. American Mathematical Society, Providence, R.I., 2004.
 - [8] E. W. Weisstein. "Prime Counting Function", "Modular Prime Counting Function", "Equinumerous", "Chebyshev Bias", "Prime Quadratic Effect". URL <http://mathworld.wolfram.com>.
 - [9] E. W. Weisstein. *CRC Concise Encyclopedia of Mathematics*. Chapman and Hall / CRC Press, 2nd ed edition, 2002.
 - [10] J. I. Latorre and G. Sierra. Quantum Computation of Prime Number Functions. 2013. URL <http://arxiv.org/abs/1302.6245>.
 - [11] J. I. Latorre and G. Sierra. There is entanglement in the primes. 2014. URL <http://arxiv.org/abs/1403.4765>.
 - [12] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.
 - [13] M. Le Bellac. *A Short introduction to quantum information and quantum computation*. Cambridge University Press, Cambridge, 2006.
 - [14] G. Benenti, G. Casati, and G. Strini. *Principles of quantum computation and information*. World Scientific, Singapore, 2004.
 - [15] E. Ribas Fernández. Simulation of the QFT of a Prime State, 2016. URL <https://github.com/kterf/QFTPrimeState>.
 - [16] S. Popescu, T. Spiller, and H. Lo. *Introduction to quantum computation and information*. World Scientific, Singapore, 1998.
 - [17] E. Aparicio Bernardo. *Teoría de los números : curso básico*. Servicio Editorial de la Universidad del País Vasco, Bilbao, 1993.