Quantum Computation of Prime Number Functions

José I. Latorre[1] and Germán Sierra[2]

[1] Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Barcelona, Spain, Centre for Quantum Technologies, National University of Singapore, Singapore.
[2] Instituto de Física Teórica UAM/CSIC, Universidad Autónoma de Madrid, Cantoblanco, Madrid, Spain.

We propose a quantum circuit that creates a pure state corresponding to the quantum superposition of all prime numbers less than 2^n, where n is the number of qubits of the register. This *Prime* state can be built using Grover's algorithm, whose oracle is a quantum implementation of the classical Miller-Rabin primality test. The *Prime* state is highly entangled, and its entanglement measures encode number theoretical functions such as the distribution of twin primes or the Chebyshev bias. This algorithm can be further combined with the quantum Fourier transform to yield an estimate of the prime counting function, more efficiently than any classical algorithm and with an error below the bound that allows for the verification of the Riemann hypothesis. We also propose a *Twin Prime* state to measure the number of twin primes and another state to test the Goldbach conjecture. Arithmetic properties of prime numbers are then, in principle, amenable to experimental verifications on quantum systems.

I. INTRODUCTION

Prime numbers are central objects in Mathematics and Computer Science. They appeared dramatically in Quantum Computation through the Shor's algorithm, which converts the hard problem of factorization into a polynomial one using quantum interference[1,2]. In Number Theory, prime numbers are fully characterized by the prime counting function $\pi(x)$, which is the number of primes less or equal to x. This is a stepwise function which jumps by one whenever x is a prime. For example $\pi(100) = 25$ means that there are 25 primes below or equal to 100, but $\pi(101) = 26$ because 101 is a prime. The asymptotic behavior of $\pi(x)$ is given by the Gauss law $\pi(x) \sim \mathrm{Li}(x)$, where $\mathrm{Li}(x)$ is the logarithmic integral function, which for large values of x behaves as $x/\log x$[3]. This statement is known as the Prime Number Theorem (PNT). Moreover, the fluctuations of $\pi(x)$ around $\mathrm{Li}(x)$, will be of order $\sqrt{x}\log x$, if and only if the Riemann hypothesis holds true[3]. Other interesting number theoretical functions are $\pi_k(x)$ which gives the number of primes $p \leq x$, such that $p + k$ is also a prime. In particular, the function $\pi_2(x)$ counts the number of twin primes. According to a famous conjecture due to Hardy and Littlewood, $\pi_k(x) \sim 2C_k\, x/(\log x)^2$ for $x \gg 1$[4], where C_k is a k-dependent constant.

The aim of this paper is to show that the number theoretical functions $\pi(x), \pi_k(x)$ and others, can be computed in an efficient way using quantum entanglement as the main computational resource. In our approach, prime numbers are represented by quantum objects which are treated as a whole with the computational tools provided by spins, photons, ions, or other quantum devices. The results we obtain suggest that difficult number theoretical problems could be addressed experimentally, once large scale quantum computation becomes available.

II. THE PRIME STATE

Our starting point is the *Prime* state made of n-qubits that corresponds to the quantum superposition of all prime numbers less than 2^n (we take $n > 1$ so that 2^n is not a prime),

$$|\mathbb{P}_n\rangle \equiv \frac{1}{\sqrt{\pi(2^n)}} \sum_{p\in \text{primes}<2^n} |p\rangle \ , \tag{1}$$

where each prime number can be expressed in binary form $p = p_0 2^0 + p_1 2^1 + \ldots + p_{n-1}2^{n-1}$, and is then translated into a quantum register on the computational basis $|p\rangle = |p_{n-1}, \ldots, p_1, p_0\rangle$. Note that all the states in the sum are orthogonal and that the normalization of the state is related to the squared root of the number of primes less than 2^n, namely $\pi(2^n)$.

As an example consider the case of $n = 3$. Then

$$\begin{aligned} |\mathbb{P}_3\rangle &= \frac{1}{\sqrt{4}}\left(|2\rangle + |3\rangle + |5\rangle + |7\rangle\right) \\ &= \frac{1}{2}\left(|\uparrow\downarrow\uparrow\rangle + |\uparrow\downarrow\downarrow\rangle + |\downarrow\uparrow\downarrow\rangle + |\downarrow\downarrow\downarrow\rangle\right). \end{aligned} \tag{2}$$

where the qubits $|0\rangle$ and $|1\rangle$ are described by the spin polarized states $\uparrow$ and $\downarrow$ of a spin 1/2 particle. Other physical realizations of qubits are of course equivalent.

Several questions arise regarding the *Prime* states: *i*) how to prepare them, *ii*) how to compute the functions $\pi(2^n), \pi_k(2^n)$, etc, *iii*) what are their entanglement properties, and *iv*) are there Hamiltonians whose ground states are $|\mathbb{P}_n\rangle$. These questions will be answered below combining standard methods in Quantum Computation and Number Theory.

The answer to question *iv*) can be readily given. It is just sufficient to take as Hamiltonian any primality test algorithm that, acting on an integer x, returns a zero for prime numbers and any positive eigenvalue λ_x for composite numbers, that is

$$\begin{aligned} H_{\text{primality}}|x\rangle &= 0 \qquad \text{if } x \in \mathbb{P}, \\ H_{\text{primality}}|x\rangle &= \lambda_x|x\rangle \qquad \text{if } x \notin \mathbb{P}, \end{aligned} \tag{3}$$

where $\mathbb{P} = \mathbb{P}_\infty$ denotes the set of all prime numbers.

A more relevant approach consists in turning a classical primality test algorithm into a quantum circuit $U_{\text{primality}}$ that is capable of discriminating prime from composite numbers

$$U_{\text{primality}} \sum_{x=0}^{2^n-1} |x\rangle|0> = |\mathbb{P}_n\rangle|0> + A \sum_{c\in\text{composite}} |c> |\lambda_c\rangle \ , \tag{4}$$

where the ancilla $|\lambda_c\rangle \neq |0\rangle$, A is a normalization constant and the explicit construction of an example of $U_{\text{primality}}$ will be presented later on. It is then possible to create the *Prime* state by performing a measurement of the ancilla. The probability to project onto the *Prime* state is given by the probability of measuring 0 on the ancilla register,

$$\text{Prob}(|\mathbb{P}_n\rangle) = \frac{\pi(2^n)}{2^n} \sim \frac{1}{n \log 2}, \tag{5}$$

where we have used the PNT, which shows the efficiency of the algorithm, since the probability to obtain the Prime state is only polinomially suppressed.

As a result, we may argue that this circuit brings the possibility of measuring $\pi(2^n)$. It is enough to repeat the preparation and keep the statistics of the output for the ancilla measurement. Even though the circuit is efficient, it shares the same complexity as a classical computer trying to assess the value of $\pi(2^n)$. However, conceptually the two approaches are quite different. On a classical computer every time we create a number, and test for primality, we simply get one prime number or none. Instead, the quantum circuit creates the superposition of all primes. This allows for the *Prime* state to be further used to explore the distribution of prime numbers. We shall show later that there is a more efficient method to create and analyze the *Prime state*, using a combination of a quantum oracle for primality and the Quantum Fourier Transform.

III. TWIN PRIMES AND GOLDBACH CONJECTURE

The construction of the *Prime* state can be generalized in a straightforward way to states that encode important concepts and problems in Number Theory. Let us start with a very simple circuit that checks for twin primes. Consider creating the prime state, and then adding 2 to each prime

$$U_{+2}|\mathbb{P}_n\rangle = \sum_{p\in\text{primes}<2^n} |p+2\rangle \tag{6}$$

We then act again with the basic primality circuit

$$U_{\text{primality}} \sum_{p:\text{primes}<2^n} |p+2\rangle|0\rangle = A \sum_{q\in\text{primes}<2^n} |q\rangle|0\rangle + B \sum_{c\in\text{composite}<2^n} |c\rangle|\lambda_c\rangle \tag{7}$$

When measuring the ancilla, the probability of finding a prime which is twin of a previous prime is

$$\text{Prob}\left((p, p+2) \in \text{primes}\right) = \frac{|A|^2}{\pi(2^n)} \tag{8}$$

On the other hand, this probability is given by the ratio

$$\text{Prob}\left((p,p+2)\in\text{primes}\right)=\frac{\pi_2(2^n)}{\pi(2^n)} \tag{9}$$

where $\pi_2(x)$ is the counting function for twin primes below or equal to x. Using the Hardy-Littlewood conjecture the ratio (9) has $O(1/n)$. Given that the production of the Prime state is itself supressed by a factor $1/n$, the global probability of measuring twin primes experimentally is expected to be $1/n^2$. This matches the same difficulty as computing the density of twin primes on a classical computer.

It is also possible to create a circuit that tests the Golbach conjecture, which states that every even integer greater that 2 can be expressed as the sum of two primes. Excluding the case $4=2+2$, one can formulate this conjecture saying that every even integer greater than 4 can be written as the sum of two odd primes. The first case being given by $6=3+3$. To formulate the Goldbach conjecture in Quantum Mechanics we shall define the state associated to odd prime numbers

$$|\mathbb{P}_{\text{odd},n}\rangle=\frac{1}{\sqrt{\pi(2^n)-1}}\sum_{2<p<2^n}|p\rangle\ , \tag{10}$$

where the summation is restricted to odd prime numbers less than 2^n. Consider now the creation of a product state of two odd Prime states, and apply a sum operation

$$|\text{Goldbach}_n\rangle\equiv U_+\left(|\mathbb{P}_{\text{odd},n}\rangle|\mathbb{P}_{\text{odd},n}\rangle\right)=\frac{1}{\pi(2^n)-1}\sum_{(p,q)\in\text{odd primes}<2^n}|p\rangle|p+q\rangle\ . \tag{11}$$

This circuit puts on the second register the addition of two odd primes. The state on the RHS uses a register with $2n+1$ quits. The reason being that the sum of two numbers between 0 and 2^n-1 runs up to $2^{n+1}-2$, so $n+1$ digits are required to store the result, which added to the n qubits for the first register gives $2n+1$.

The sum $p+q$ is an even number greater or equal to 6. The Goldbach conjecture asserts that all the even numbers will appear in the second register of (11) for sufficiently large values of n. Again, this strategy does not bring any improvement over a classical strategy but is conceptually different since the second register contains the superposition of all even numbers.

IV. ENTANGLEMENT OF THE PRIME STATE

The *Prime* state must carry a large amount of quantum entanglement. Otherwise, it would be possible to simulate it on a classical computer with polynomial resources. A good figure of merit to quantify the entanglement present in the *Prime* state is the von Neumann entropy for the reduced density matrix of a subsystem. To be concrete, we first divide the system in the first l qubits and the rest $n-l$ qubits. Then the reduced density matrix

$$\rho(l)=\text{Tr}_{n-l}|\mathbb{P}_n\rangle\langle\mathbb{P}_n|, \tag{12}$$

is computed. Finally we calculate the entanglement entropy

$$S\left(\rho(l)\right)=-\text{Tr}_l\rho(l)\log\rho(l). \tag{13}$$

There are two relevant properties of the von Neumann entropy of the *Prime* state. First, we fix the size of the register n and we observe that the entropy grows approximately as $\log l$. Second, we consider the even bi-partition of the system $l=n/2$, with n even, and explore how the entropy $S(\rho(n/2))$ varies with n. The entropy can be seen to clearly scale *almost* in the maximal way, that is linearly in n. Both results have been obtained from exact numerical simulations up to $n=22$.

An interesting question is how single qubits are entangled with the rest of the qubits in the *Prime* state. This is described by the reduced density matrices

$$\rho^{(i)}=\text{Tr}_{n/i}\,|\mathbb{P}_n\rangle\langle\mathbb{P}_n|,\quad i=0,1\ldots,n-1, \tag{14}$$

where the trace excludes the i^{th} qubit. For the last qubit, $i=0$, one finds

$$\rho^{(0)}_{0,0}=\frac{1}{\pi(N)},\rho^{(0)}_{1,1}=\frac{\pi(N)-1}{\pi(N)},\rho^{(0)}_{0,1}=\frac{1}{\pi(N)}, \tag{15}$$

where $N = 2^n$. For a large number of qubits n, the PNT implies that the entanglement entropy of the last qubit decreases exponentially with n

$$S_0 = -\mathrm{Tr}\,\rho^{(0)}\,\log\,\rho^{(0)} \sim 2^{-n}(n\log 2)^2. \tag{16}$$

The reason being that all the primes but 2 are odd, so the last qubit is mostly in the state $p_0 = 1$. A more interesting result is obtained for the next to last qubit, $i = 1$, whose density matrix is

$$\rho^{(1)}_{0,0} = \frac{\pi_{4,1}(N)}{\pi(N)}, \rho^{(1)}_{1,1} = \frac{1+\pi_{4,3}(N)}{\pi(N)}, \rho^{(1)}_{0,1} = \frac{\pi^{(1)}_2(N)}{\pi(N)}, \tag{17}$$

where $\pi_{a,b}(x)$ is the number of primes less or equal to x that appear in the arithmetic progression $am+b$, with a and b coprime numbers, and $\pi^{(1)}_2(x)$ is the number of prime pairs $(p, p+2)$ less or equal to x with $p = 1 \bmod 4$. There are also prime pairs with $p = 3 \bmod 4$, in number $\pi^{(3)}_2(x)$, but they do not contribute to $\rho^{(1)}_{0,1}$. The sum $\pi^{(1)}_2(x) + \pi^{(3)}_2(x)$ is equal to the twin primes counting function $\pi_2(x)$. Dirichlet proved that the number of primes in these arithmetic progressions is infinite[3]. Furthermore, the fraction of these primes relative to the total number of primes satisfies a version of the PNT,

$$\lim_{x\to\infty} \frac{\pi_{a,b}(x)}{\mathrm{Li}(x)} = \frac{1}{\phi(a)} \tag{18}$$

where $\phi(a)$ is the Euler totient function, which is the number of positive integers $x < a$ which are relative prime to a. Using this result and the fact that $\phi(4) = 2$, one finds that the entanglement entropy of the qubit $i = 1$ behaves asymptotically as

$$S_1 = -\mathrm{Tr}\,\rho^{(1)}\,\log\,\rho^{(1)} \sim \log 2, \qquad n \gg 1. \tag{19}$$

So this qubit is maximally entangled with the rest. The same property holds for the remaining qubits. The reduced density matrices $\rho^{(i)}$ also provide the expectation values of local operators in the *Prime* state. In particular for the Pauli matrices σ^a_i one has

$$\langle\sigma^a_i\rangle = \mathrm{Tr}\,(\rho^{(i)}\sigma^a_i), \quad a = x, y, z, \quad i = 0, \ldots, n-1. \tag{20}$$

For example the magnetization of the qubit $i = 1$ reads

$$\langle\sigma^z_1\rangle = \frac{\pi_{4,1}(N) - \pi_{4,3}(N) - 1}{\pi(N)}. \tag{21}$$

The numerator is essentially the Chebyshev bias[5]

$$\Delta(x) = \pi_{4,3}(x) - \pi_{4,1}(x), \tag{22}$$

which counts the unbalance of the remainder upon dividing a prime by 4. For low values of x, the remainder 3 appears more often than the remainder 1, but Hardy and Littlewood showed that the relative size of $\pi_{4,3}(x)$ and $\pi_{4,1}(x)$ vary infinitely often so that $\Delta(x)$ can be either positive or negative[5]. This result, known as the prime quadratic effect, could be observed experimentally by measuring $\langle\sigma^z_1\rangle$. Similarly, the twin prime functions $\pi^{(1,3)}_2(N)$ are the expectation values of one and two sites spin flips operators,

$$\langle\sigma^x_1\rangle = \frac{2\,\pi^{(1)}_2(N)}{\pi(N)}, \quad \langle\sigma^x_1\sigma^x_2 + \sigma^y_1\sigma^y_2\rangle = \frac{4\,\pi^{(3)}_2(N)}{\pi(N)}. \tag{23}$$

In analogy with eq.(22) we can define the twin prime bias $\Delta_2(x) = \pi^{(3)}_2(x) - \pi^{(1)}_2(x)$, which seems also to oscillate.

V. PRIMALITY QUANTUM ORACLE

A different way to prepare the *Prime* state corresponds to use a primality module as an oracle in Grover's algorithm[6]. We are searching for $M = \pi(2^n)$ items (the primes below 2^n) within a set of $N = 2^n$ objects (the integers between

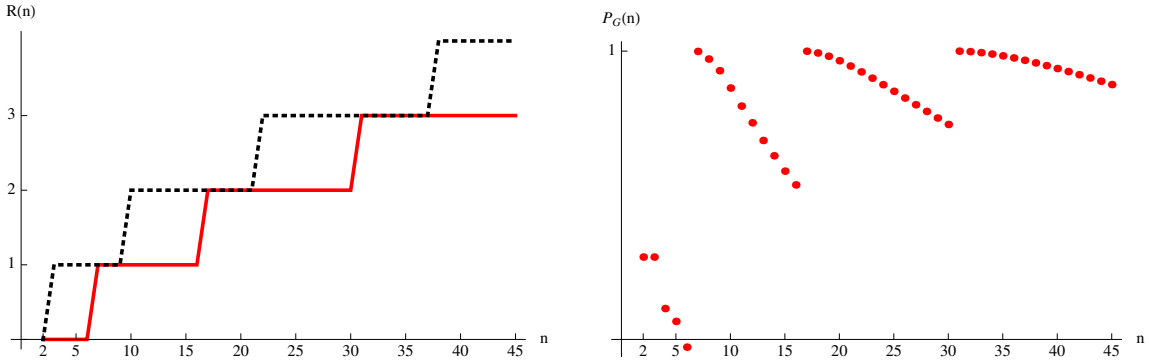

FIG. 1: Left: Number of Grover's steps needed to create the *Prime* state $|\mathbb{P}_n\rangle$ in the range $n = 2, \ldots, 45$ ($R(n)$: continuous line and $R_{\max}(n)$: dashed line). Right: Accuracy of the state measured by $P_G(n)$.

0 and $2^n - 1$). Using the Grover's algorithm, on a quantum computer, this search can be performed in $O(\sqrt{N/M})$ steps with a high probability, which represents a significant computational gain[2].

As oracle for the Grover's algorithm we use the unitary transformation

$$U_f|x\rangle = (-1)^{f(x)}\ |x\rangle \tag{24}$$

where $f(x) = 1$ if $x \in \mathbb{P}_n$ and $f(x) = 0$ if $x \notin \mathbb{P}_n$. One next introduces the unitary $U_\psi = 2|\psi\rangle\langle\psi| - \mathbf{1}$, where $|\psi\rangle = N^{-1/2}\sum_{x=0}^{N-1}|x\rangle$ is the state obtained applying n Hadamard transforms to the initial state $|0\rangle^{\otimes n}$. Grover's transformation, defined as $G = U_\psi U_f$, is applied iteratively to the state $|\psi\rangle$ until it gets closed to the target state $|\mathbb{P}_n\rangle$. The optimal value of iterations, $R(n)$, is estimated by

$$R(n) = \left[\frac{\arccos\left(2^{-n/2}\sqrt{\pi(2^n)}\right)}{2\arcsin\left(2^{-n/2}\sqrt{\pi(2^n)}\right)}\right] \tag{25}$$

where $[x]$ denotes the integer part of x. If $M \leq N/2$, as it occurs in our problem, there is an upper bound

$$R(n) \leq \left[\frac{\pi}{4}\sqrt{\frac{N}{M}}\right] \leq R_{\max}(n) \equiv \left[\frac{\pi}{4}\sqrt{n\log 2}\right] \tag{26}$$

which follows from the PNT for $n \gg 1$. Hence the Grover's algorithm requires $O(\sqrt{n})$ calls to the oracle, which represents a computational gain compared to a classical algorithm (see Fig. 1). Note that one needs about 3 Grover's iterations to construct an approximation to the *Prime* state up to $2^{45} \sim 3.5 \times 10^{13}$!! To assess the goodness of the approximation we compute the overlap between the *Prime* state with the Grover state after $R(n)$ iterations

$$P_G(n) = |\langle\mathbb{P}_n|G^{R(n)}\ |\psi\rangle|^2 = \sin^2\left[\frac{(2R(n)+1)\theta(n)}{2}\right] \tag{27}$$

where $\theta(n)$ is the Grover's angle

$$\theta = \theta(n) = 2\arcsin\sqrt{M/N} = 2\arcsin\left(2^{-n/2}\sqrt{\pi(2^n)}\right). \tag{28}$$

The overlap (27), shown in Fig.1, has some jumps with n but it approaches 1 rather fast as n increases.

The above Grover construction relies on the fact that some classical primality tests can be turned into a quantum oracle. This is the case of the Miller-Rabin primality test which we will write down below as a quantum circuit. The remarkable AKS primality test ([7], which is unconditional, deterministic and efficient) could also be turned into an oracle. Nevertheless, the Miller-Rabin test has a simpler structure which makes easier its conversion into a quantum primality oracle.

Let us first summarize the Miller-Rabin primality test[8]. The goal is to declare a number x either prime or composite. First, it is necessary to find the integers s and d (odd) such that an odd number x is decomposed as $x - 1 = 2^s d$. We then choose a number a, in the range $1 \leq a < x$, that is called witness and check

$$\begin{aligned} &a^d \not\equiv 1 \pmod{x} \\ &a^{2^r d} \not\equiv -1 \pmod{x} \qquad 0 \leq r \leq s-1. \end{aligned} \tag{29}$$

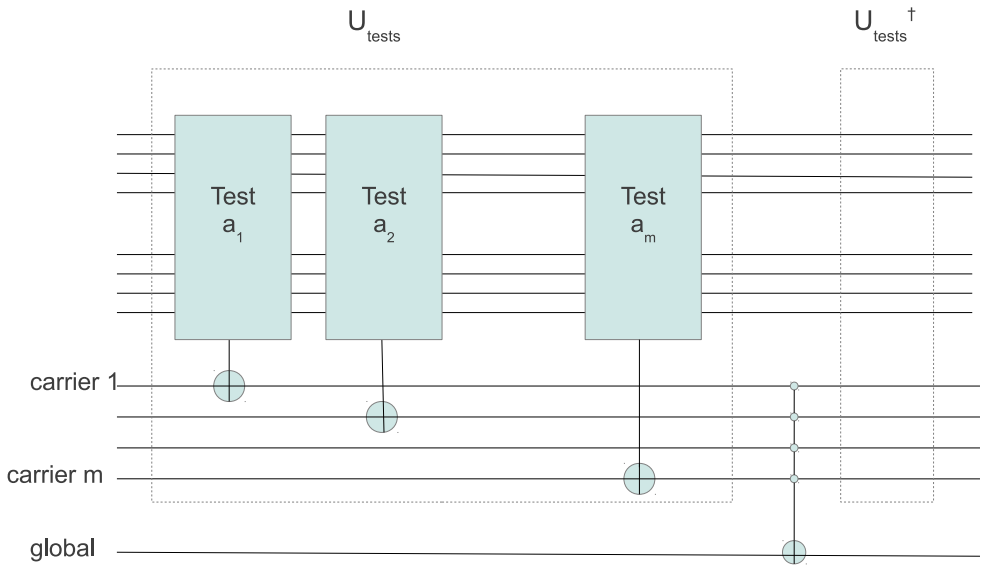

FIG. 2: Structure of the Quantum Primality Oracle based on the Miller-Rabin primality test. A series of unitary modules implement a quantum version of the modular exponentiation tests required by the classical test. The total number of tests m is smaller than n^2.

If all these tests are verified, x is composite with certainty. However if the test fails, x can be either prime or composite. In the latter case the number a is called a strong liar to x. In order to circumvent strong liars, it is necessary to rerun the test with different witnesses. As more witnesses are tested, the probability to be deceived by strong liars vanishes. Assuming the Generalized Riemann Hypothesis (GRH), the Miller-Rabin test is deterministic using less than $\log^2 x$ witnesses. For instance, all numbers below $x < 3\ 10^{14}$ can be correctly classified as prime or composite using as witnesses $a = 2, 3, 5, 7, 11, 13, 17$. We can also implement the probabilistic version of the Miller-Rabin test which does not assume the GRH and that using k witnesses declares a composite to be prime with an error less than 2^{-2k}[8]. Hence choosing k to be equal to n the error will be negligable for our purposes.

The quantum primality oracle based on the Miller-Rabin test follows closely the steps of the classical test. Basically, a series of unitary modules implement a quantum version of each of the classical modular exponentiation tests that form the Miller-Rabin test, as shown in Fig. 2. In order to simplify the algorithm, we shall consider the construction of the odd superposition in the *Prime* state, that is we leave out the element $|2\rangle$. This is a trivial element that could be restored with a simple initial controlled gate. We thus start by preparing the superposition of all odd numbers less than 2^n, using $n-1$ Hadamard operations on the first $n-1$ qubits, while leaving the last qubit set to $|x_0\rangle = |1\rangle$, and adding a set of target ancillae that will be used to implement the modular exponentiation tests

$$|\psi_0\rangle = \frac{1}{2^{(n-1)/2}} \sum_{x_{n-1},\ldots,x_1=0,1} |x_{n-1},\ldots,x_1,1\rangle|0\rangle. \tag{30}$$

For each value of $|x\rangle$ we need to find two states $|d\rangle$ and $|s\rangle$ such that $|x-1\rangle = |d\rangle|s\rangle$. This can be done using the fact that $|s\rangle$ is related to the number of trailing zeros in the register when subtracting 1, while $|d\rangle$ is related to the initial set of the qubits. Let us illustrate this fact in the case where the register reads $|25\rangle = |1,1,0,0,1\rangle$, where we have $|d\rangle = |3\rangle = |11\rangle$ (from the initial $|1,1\rangle$ piece of the register) and $s = 3$ (that is $|000\rangle$ from the trailing $|0,0,1\rangle$ minus 1, see Fig. 3). This example shows that a series of gates controlled by several qubits is enough to perform the

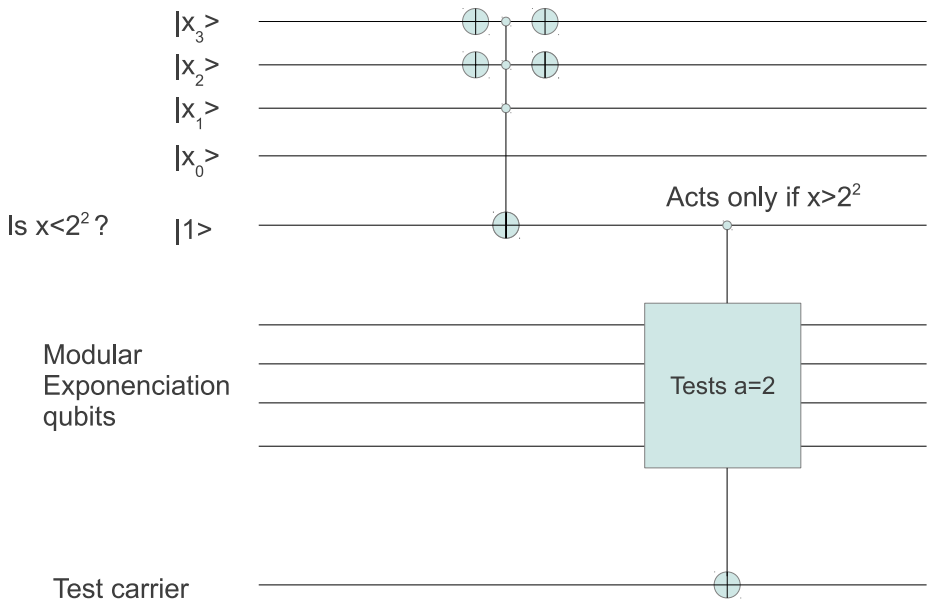

FIG. 3: Detail of the condition that guarantees that only those witnesses less than x are tested.

modular exponentiation as a unitary operation

$$U_{a,r}\sum_x |x\rangle|0\rangle = \sum_x |x\rangle|a^{2^r d}(\mathrm{mod}\, x)\rangle, \quad 0 \le r \le s-1. \tag{31}$$

Nevertheless there is a subtle detail to be considered. The Miller-Rabin test requires the witness a to be smaller than x. Fortunately, this condition also guarantees that the above operation is unitary[9]. Therefore the action of each unitary modular exponentiation needs to check that x is large enough for each witness. This again is simply taken care of by a controlled gate to the most relevant qubits in x (see Fig. 3). For instance, a gate control to the most relevant qubit in x, that is $|x_n\rangle$ will act when the qubit is $|1\rangle$, that is when $x > 2^{n-1}$ and all witnesses less than 2^{n-1} can be used. Let us here recall that the values of the witnesses in the Miller-Rabin algorithm are far smaller than the values of x they can test.

The next step in the algorithm is to collect the result of the tests. The guiding principle is to assume x is composite till proven prime. A set of ancillary carriers will be initialized in a state corresponding to *composite* unless they are changed by the result of a test, which will correspond to *prime*. Let us recall that in order for an integer x to be declared a probable prime we just need to find that $a^d = 1$ or $a^{2^r d} = -1$ for some $r \in [0, s-1)]$ (see Eq.(29)). This can be achieved quantum mechanically by adding an ancillary carrier for each test based on the witness a and the value r, that we call $\mathrm{test}_{a,r}$ such that it is initially set to $|\mathrm{test}_{a,r}\rangle = |1\rangle$, and then changed to $|0\rangle$ if the $\mathrm{test}_{a,r}$ fails detecting a probable prime,

$$U_{\mathrm{test}_{a,r}}|a^{2^r d}\,(\mathrm{mod}\, x)\rangle|0\rangle = |a^{2^r d}\,(\mathrm{mod}\, x)\rangle|\mathrm{test}_{a,r}\rangle\ . \tag{32}$$

After the action of all tests, all ancillae carriers will be $|1\rangle$ only for composite numbers, and will have at least one $|0\rangle$ for prime numbers. This suggests to include a single extra global ancilla that summarizes all tests, initialized to $|1\rangle$.

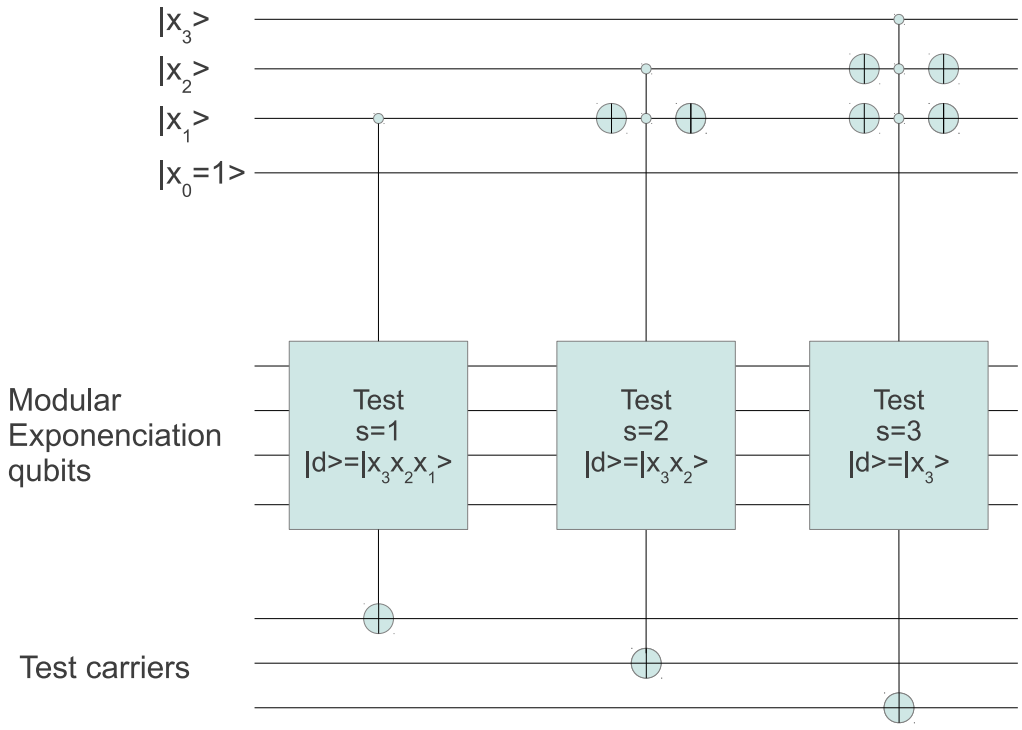

FIG. 4: Implementation of $x-1=d2^s$ on a quantum circuit. The value of s is inferred by the trailing zeros in the register, while d is read from the leading qubits. Each test result is retained in its corresponding carrier. All carriers will be later collect into a single global one.

We then perform a 3-body gate U_{global} controlled to all test ancillae displayed in Fig. 4

$$U_{\text{global}} \prod_{a,r} |\text{test}_{a,r}\rangle|1\rangle = \prod_{a,r} |\text{test}_{a,r}\rangle|\text{global}\rangle \tag{33}$$

If x is prime, the *global* ancilla will flip to $|0\rangle$, and if x is composite it will remain in the state $|1\rangle$. This is precisely what we need to implement the Grover condition in the usual way using a single state.

To finish the algorithm, after the Grover sign flip on primes is achieved, we need to invert all the unitary operations so as to reset all ancillae to their initial product state.

The computational complexity of the Miller-Rabin quantum oracle is only polynomial. We can bound the number of basic operations in the following way. There are at most n^2 witnesses to be tried. Each witness needs at most n exponential tests. Each test is of order n^3 operations. Altogether, the oracle complexity scales as n^6. This counting assumes that some test carriers and control operations to guarantee that $a < x$ are done using single Toffoli-like gates. Note that, as a matter of fact, the number of witnesses needed in practice is lower than the n^2 bound proven using the Generalized Riemann hypothesis. Therefore, the algorithm will work in a faster way in practice.

VI. QUANTUM COUNTING OF PRIME NUMBERS

The power of the Grover algorithm becomes manifest when it is combined with the efficient quantum Fourier transform. The Quantum Counting algorithm[10] is based on the idea that the Grover module is followed by an appropriate controlled phase gate in such a way that, after completion of the series of calls to the oracle, a quantum Fourier transform is performed to read the number of solutions to the oracle.

In our case, the Quantum Counting algorithm that makes use of our Grover primality oracle allows to compute the number of solutions $\pi(x) = \pi(2^n) = M$ with a bounded error. To be precise, it will produce an estimate $\tilde{M}$ to the actual number of solutions M to the oracle such that

$$\left|\tilde{M} - M\right| < \frac{2\pi}{c} M^{1/2} + \frac{\pi^2}{c^2}, \tag{34}$$

where c is a constant, using only $c\,N^{1/2} = c\,x^{1/2}$ calls to the oracle, that is time steps. Given that $\pi(x) \sim x/\log x$, our quantum algorithm can verify the prime counting function with an accuracy

$$|\tilde{\pi}(x) - \pi(x)| < \frac{2\pi}{c} \frac{x^{1/2}}{\log^{1/2} x} \tag{35}$$

and $O(n = \log(x))$ space allocation.

These results provide an exponential gain with respect to known classical algorithms, when considering the need for both time and memory resources. The classical computation of $\pi(x)$ of use was proposed by Lagarias, Miller, and Odlyzko[11], who refined the Meissel-Lehmer method. The number of bit operations is of order $x^{2/3}$ and the storage needed is of order $x^{1/3}$, where both scalings have log corrections. Lagarias and Odlyzko have also proposed two analytic $\pi(x)$-algorithms based on the Riemann zeta function, whose order in time and space are $x^{3/5+\epsilon}$ ($\epsilon > 0$) and x^{ϵ} in one case, and $x^{1/2+\epsilon}$ and $x^{1/4+\epsilon}$ in the other case[12]. The latter algorithms has been implemented numerically to compute $\pi(10^{24})$ unconditionally[13]. Classically, it is possible to find other algorithms that trade space with time, yet the product of time and memory is always bigger than order $x^{1/2}$. The estimation of $\pi(x)$, given by eq.(35), is smaller than the error predicted under the Riemann hypothesis (RH), i.e. $|\pi(x) - \mathrm{Li}(x)| < O(\sqrt{x}\log x)$, thus the RH could be falsified experimentally on a quantum computer with numbers far beyond the reach on any classical computer. However, the proof of the RH cannot be achieved using this method since that would require testing systems of arbitrary size.

VII. CONCLUSION

We have shown that the quantum superposition of states that codify prime numbers in the computational basis, the *Prime* state, can be created efficiently using a quantum circuit for primality test. A similar efficient construction can be done in terms of a *Twin Prime* state, that provides the grounds for experimental counting of twin primes. The *Prime* state can also be used to verify Goldbach conjecture. The entanglement properties of the *Prime* state are directly related to counting functions of subseries of prime numbers, such as twin primes. Furthermore, the combination of a quantum circuit for primality test and the Quantum Fourier Transform allows for a counting of prime numbers within an error which is smaller to the fluctuations allowed by the Riemann Hypothesis.

The entanglement properties of the *Prime* state remain to be explored in more detail. It is likely that the quantum correlations emerging from the *Prime* state are profoundly related to theorems in Number Theory.

Acknowledgements. The authors are grateful to J. I. Cirac, A. Córdoba and S. Iblisdir for helpful comments. J. I. L. acknowledges financial support from FIS2011-16185, Grup de Recerca Consolidat ICREA-ACADÈMIA, and National Research Foundation & Ministry of Education, Singapore; and G. S. from the grants FIS2012-33642, QUITEMAD and the Severo-Ochoa Program.

---

[1] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[3] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York (1980).
[4] G. H. Hardy and J. E. Littlewood, Acta Math., **44**, 1 (1923).
[5] B. C. Berndt, *Ramanujan's Notebooks, Part IV*, New York, Springer-Verlag, 135 (1994).
[6] L. K. Grover, Proc. 28th Annual ACM Symposium on Theory of Computing (1996).
[7] M. Agrawal, N. Kayal and N. Saxena, Annals of Maths **160** 781 (2004).
[8] G. L. Miller, J. Comp. and Sys. Sciences. **13**, 300 (1976); M. O. Rabin, J. of Number Theory **12**, 128 (1980).
[9] V. Vedral, A. Barenco and A. Ekert, Phys. Rev. A **54**, 147 (1996).
[10] G. Brassard, P. Høyer and A. Tapp, ICALP'98, Springer-Verlag, LNCS **1443**, 820 (1998).
[11] J. C. Lagarias, V. S. Miller and A. M. Odlyzko, Math. Comp. **44**, 537 (1985).
[12] J. C. Lagarias and A. M. Odlyzko, J. Algorithms **8**, 173 (1987).
[13] D. J. Platt, arXiv:1203.5712.