A Realizable Quantum Simulator of the Integer Factorization Problem

Jose Luis Rosales* and Vicente Martin†
Center for Computational Simulation (Madrid)
DLSIIS ETS Ingenieros Informáticos,
Universidad Politécnica de Madrid,
Campus Montegancedo, E28660 Madrid.
(Dated: July 8, 2017)

We study the problem of decomposing a number into its prime factors, $N = xy$, using a quantum simulator. First, we derive the Hamiltonian of the physical system that simulates a new arithmetic function formulated for the factorization problem that represents the energy of a quantum computer. We solve the spectrum of the quantum system showing that it obtains, for $x \ll \sqrt{N}$, a prediction of the prime counting function that is almost identical to Riemann's $R(x)$. We also introduce a physical realization of the simulator consisting in preparing a Bell state for two electrons in a Penning trap. The outcome of the simulator will be the histogram of the measured energies of the simulator. Only $o(\log\sqrt{N})^3$ energy measurements are required to characterize a probability distribution for the factors of N; this is similar to Shor's algorithm complexity for the same problem using quantum mechanics. It allows to infer the likelihood for a prime to factorize N.

The relevance of this work for network communications lies on the fact that a quantum computer of this kind will jeopardize the security of the widely used cryptography systems in conventional communication networks, which relies on the classical intractability of the factorization problem. Hence, since quantum cryptography (with continuous or discrete variables) is now becoming a paradigm of secure communications, the work intends to demonstrate the urgency to migrate to quantum security.

EXTENDED ABSTRACT

The factorization problem is one of the biggest unsolved problems in computer science: a classical computer, using the best factoring algorithms known at present [1], requires an exponentially large number of steps to find the primes factors of an l-digit integer N. However, following the principles of quantum mechanics, a computer will obtain the factors of $N = xy$ in polynomial time using Shor's algortithm [3], a fact that will jeopardize the security of the widely used cryptography systems in conventional communication networks, which relies on the classical intractability of this problem [2]. The exponential speed up of quantum algorithms is due to the interference of probability amplitudes for the prepared states during unitary evolution. Nonetheless, the construction of a fully programmable quantum computer running Shor's algorithm is still a significant experimental challenge because it requires coherent control over many qubits. The alternative shown here is to build the solutions of the problem in the Hilbert space of a quantum simulator performing factorization instead of going through the route of a gate-based, fully programmable, quantum computer. The key idea is to translate factoring arithmetics into the physics of a device whose superposition of states mimics the problem: i.e., a factoring (analog)computer.

Having this in mind, we have recently proposed an equivalent formulation of the factorization problem where the issue of finding the factor x is replaced by that of reaching the value of a new function E, depending on x [4]. The new formulation is adequate to finding the probability distribution of $E(x)$ within a finite, well defined, ensemble of pairs of prime numbers which is univocally determined for any N. Since every possible factor of N belongs to this set, we called it the factorization ensemble. Additionally, owing to the statistical properties of $E(x)$ in this set (see [4] and [5]), the histogram of the computed eigenvalues infers a measure of the quantum probability for a given x to be a factor of N.

The new formulation is thus translated into the physics of a system with bounded trajectories that, using semiclassical quantization, could be interpreted as the classical counterpart of a quantum factoring simulator when E is identified with the energy. This approach will be correct for very large N which, indeed, is the more relevant and practical case.

In this work we also propose a physical realization for the physical state of the quantum simulator which, as a matter of fact, is achievable with the current technology: A Cooper pair in a Penning Trap. The measurement of only $o(\log\sqrt{N})^3$ magnetron frequencies will provide the location of the more likely factors $x = o(\sqrt{N})$ (see also [5] for details on how the simulator operates).

Let us then define the factorization ensemble $\mathcal{F}(j)$ as the set of all primes x_k and y_k such that when multiplied obtain numbers N_k, in a vicinity of N, with the property $\pi(\sqrt{N_k}) = \pi(\sqrt{N}) = j$. Now, for each x_k and y_k such that $N_k = x_k y_k$ in the ensemble, a bijection with x_k is defined with the function

$$E_k = \pi(x_k)\pi(y_k)/j^2. \tag{1}$$

From these definitions, the set (E_k, N_k) can be calcu-

* Jose.Rosales@fi.upm.es
† Vicente@fi.upm.es

lated and depicted, e.g., in Fig. 1. As a matter of fact, it shows the typical band structure of the energy spectrum of a quantum device. On the other hand, this kind of behavior for an arithmetic function of the primes in the ensemble can not be deduced from its definition in number theory.

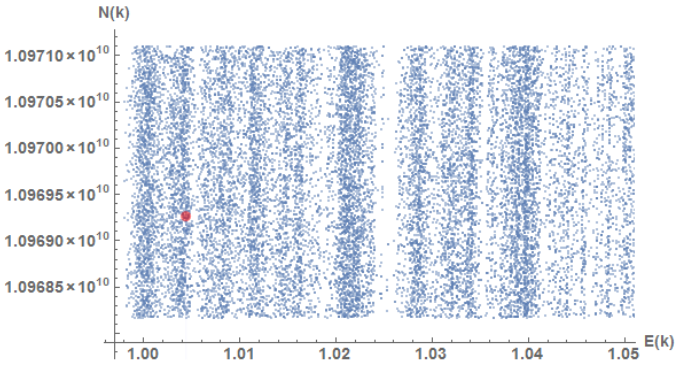

FIG. 1. A plot of the pairs of values (E_k, N_k) in $\mathcal{F}(10000)$. The point, e.g., $N = 10969262131 = 47297 \cdot 231923$, $E = 1.00441815$ is represented (in red).

Now define the canonical variables $q = (\pi(x)+\pi(y))/2j$ and $p = (\pi(y) - \pi(x))/2j$, for $x < y$. Then Eq. 1 transforms into the function

$$E(p, q) = -p^2 + q^2. \tag{2}$$

For $x, y \in \mathcal{F}(j)$ it corresponds to the energy of a bounded hamiltonian. Given that the possible energies belong to a finite set, we are allowed to build a normalizable quantum amplitude $\Psi(q)$ satisfying the Schödinger equation if we assume the quantum conditions $[p, q] = i\hbar$

$$\Psi'' + q^2\Psi = E\Psi. \tag{3}$$

The solutions are stationary waves. Moreover, self-consistency with number theory can be obtained if and only if the cardinal of the factorization ensemble coincides with the dimension of the Hilbert space.

Results. In [4], for large quantum numbers, we obtained the eigenvalues $\{E_k\}$ leading, as a corollary, to calculate an asymptotic approximation for the prime counting function $\pi_Q(x)$ that, although explicitly depends about the number N, it actually provides the same results for all the numbers used so far for computation, a fact that must be related to the universality of the primes as possible factors of a given number and that is here obtained purely from quantum mechanics. The exactitude of the quantum derived prime counting function is tantamount to the approximation calculated by Riemann $R(x)$ as seen in Fig. 2.

Moreover we have also obtained the solution of the quantum conditions of the simulator [5]

$$E_k(\mathcal{G}) \simeq 1 + 1/\log q_{\mathcal{G}} \cdot \frac{2\pi}{k_m} k + o(k/k_m)^2, \tag{4}$$

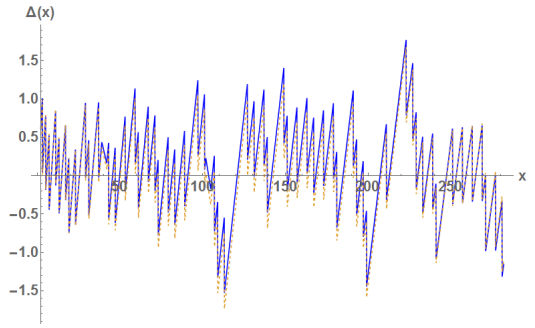

FIG. 2. The functions $\Delta_Q = \pi(x) - \pi_Q(x)$ calculated here (blue) and $\Delta_R = \pi(x) - R(x)$ (dashed orange) for e.g., $x \in \mathcal{F}(3155)$.

where $q_{\mathcal{G}}$ is a zero of the wave function of the simulator with the boundary condition $\Psi(1) = 0$, (which corresponds to primes $x = o(\sqrt{N})$). Here, $k_m \sim \frac{3}{2}\pi(\log\sqrt{N})^3$, must be the number of stationary states of the simulator which only scales polynomially with the number of digits of N. Each of the zeroes of $\Psi(q)$ define a gauge related to the actual size of the device and, given its arbitrariness, a statistical average can be determined. The results are summarized in Figs. 3 (quantum theoretical) and 4 (actual number theoretical). The probability for a prime $x(E)$, to be a factor or N is higher in the red area and becomes zero in the blue regions. There exists a pretty reasonable concordance between both graphics. Recall that both plots are exactly normalized because we represented $(\log\sqrt{N})^3$ points in both graphics.

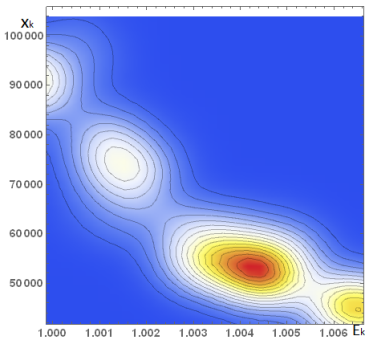

FIG. 3. Density plot for the distribution of values (E_k, x_k) calculated quantum mechanically for the simulator of $\mathcal{F}(10000)$.

We finally introduced in [5] a physical realization of the simulator, with the same eigenvalues than that in Eq. 4, consisting in preparing a Bell state for two electrons in a Penning trap. The physical parameters or the trap depend on the number N we are intended to factorize. The histogram of the measured energies corresponding to the magnetron motion provides a measure of the probability of a given prime to be a factor of N. When the measured arithmetic function E is fed into a classical sieve we should obtain an exponential speed up because, by construction, the expected linear jumps in $E(x)$ lead to

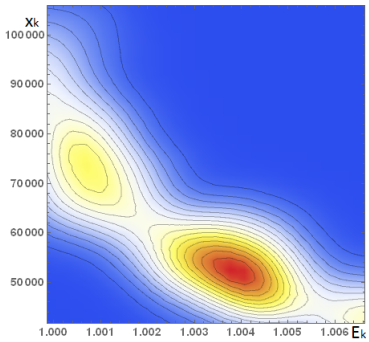

FIG. 4. Actual density plot for the distribution of values (E_k, x_k) for the primes in $\mathcal{F}(10000)$.

exponential ones in x. Our results should be thus similar to the expected ones using Shor's algorithm but without actually requiring a gate-based quantum computer. Recall that noise can strongly affect the exactitude of magnetron frequencies measurements in a Penning Trap [6].

For electron traps with radius $\varrho_m \sim 3$ mm [6], numbers up to $N \leq 10^{20}$ can be factorized with the quantum simulator. While these are still far from RSA-sized numbers, they are many orders of magnitude larger than what has been demonstrated up to now.

This work has been partially supported by Comunidad Autónoma de Madrid, project Quantum Information Technologies Madrid, QUITEMAD+ S2013-IC2801 and by project CVQuCo, Ministerio de Economa y Competitividad, Spain, Project No. TEC2015-70406-R. MINECO/FEDER UE.

[1] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective (Springer, New York, 2001), ISBN 0-387-94777-9.
[2] Koblitz, N. (1994) "A Course in Number Theory and Cryptography" (Springer, New York).
[3] Shor (1994), P.W. "Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA), p. 124.
[4] Rosales, J.L. and Martin, V. (2016) "Quantum Simulation of the Factorization Problem", Phys. Rev. Lett. 117, 200502
[5] Rosales, J.L. and Martin, V. (2017),"A Bell state in a Penning Trap as a quantum simulator of the factorization problem", https://arxiv.org/abs/1704.03174
[6] Brown, L.S. and Gabrielse, G. (1986), "Geonium theory: Physics of a single electron or ion in a Penning trap", Rev. Mod. Phys. 58,1, pp 233-311.