Bell states in a Penning trap as the quantum simulator of the integer factorization problem.

Jose Luis Rosales\textsuperscript{1} and Vicente Martin\textsuperscript{1}

Center for Computational Simulation (Madrid)

DLSHS ETS Ingenieros Informáticos,

Universidad Politécnica de Madrid,

Campus Montegancedo, E28660 Madrid.
(Dated: May 18, 2017)

We recently introduced a formulation of the integer factorization problem for \( N = xy \) based on the physics of a quantum device. The energies of this system, being related univocally with the factors of \( N \) in number theory, are the eigenvalues of a bounded Hamiltonian. Here we solve the quantum conditions to obtain a discrete energy spectrum that allows to assign a relative probability for a prime to be a factor candidate of \( N \). This kind of quantum sieve can be understood as a polynomial time probabilistic quantum factoring algorithm only requiring \( O(\log N)^2 \) energy measurements. Finally the state of this quantum simulator will be identified as that corresponding to two entangled electrons in a Penning trap. We also consider the possibility to build the simulator experimentally to obtain, from the measured magnetron trap frequencies, a device performing a probabilistic quantum sieve for the possible factors of \( N \).

PACS numbers: 03.67.Ac,03.67.Lx,02.10.De

A classical computer, using the best factoring algorithms known at present \cite{1}, requires a number of steps that grows exponentially with \( l \), the number of digits of \( N \), the integer to factorize. Indeed, for large numbers the intractability of the factorization problem underlies the security of cryptographic algorithms like RSA or Diffie-Hellman \cite{2}.

However, following the principles of quantum mechanics, a computer will solve the problem in polynomial time when it is programmed with Shor’s algorithm \cite{3}. The exponential speed up is due to the quantum interference of probability amplitudes for the prepared states during unitary evolution, a property of the quantum Fourier transform on which the algorithm is based. As a matter of fact, the number 15 was successfully factorized with this algorithm using a molecule serving as a seven qubits quantum computer \cite{4}. However, even for this small \( N \), preparing a fully programmable quantum computer is still a significant experimental challenge because it requires coherent control over many qubits. Resorting to the preparation and measurement of complex states embodying properties of the primes \cite{5} is also difficult and has not been realized up to now.

On the other hand, we have recently proposed an equivalent formulation of the factorization problem where the factor \( x \) is replaced by the value of a function \( E(x) \) \cite{6}. Thus, while Shor’s algorithm reproduces the outputs of an arithmetic function that is periodic, module \( N \), to find \( x \leq \sqrt{N} \), the new formulation is more adequate to find the probability distribution of \( E(x) \) within a finite ensemble of prime numbers. Since every possible factor of \( N \) belongs to this set, we called it the factorization ensemble. Moreover, owing to the statistical properties of \( E(x) \), a probability for a given \( x \) to be a factor of \( N \) could be inferred. The new formulation can be translated to the physics of a two dimensional system with bounded trajectories that, using semiclassical quantization, could be interpreted as the classical counterpart of a quantum factoring simulator if \( E \) is identified with the energy. This approach will be correct for very large \( N \) which, indeed, is the more relevant and practical case.

The factorization ensemble \cite{6} is defined as the set of all primes \( x_k \) and \( y_k \) such that their product yields numbers \( N_k \), in a vicinity of \( N \), with the property \( j = \pi(\sqrt{N_k}) = \pi(\sqrt{N}) \).

\[
\mathcal{F}(j) = \{(x_k, y_k)/ N_k = x_k \cdot y_k : \pi(\sqrt{N_k}) = j\}. \tag{1}
\]

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

\[
E_k = \frac{\pi(x_k)\pi(y_k)}{j^2}. \tag{2}
\]

Since \( E_k \leftrightarrow (x_k, y_k) \) univocally, the solution \( (x, N) \) of the factorization problem can be rewritten as the pair \( (E, N) \). Asymptotically, the prime number theorem implies that for \( x = O(\sqrt{N}) \), \( E \) scales logarithmically with the factor \( x_k \). From these definitions, the set \( (E_k, N_k) \) can be calculated. In Fig. 1 we present the results for \( j = 10000 \), showing the typical band structure of a quantum spectrum.

Now we can define the variables \( q = (\pi(x) + \pi(y))/2j \) and \( p = (\pi(y) - \pi(x))/2j \), for \( x < y \). Then Eq. (2) transforms into the inverted harmonic oscillator energy function

\[
E(p, q) = -p^2 + q^2. \tag{3}
\]

In \cite{6}, it was demonstrated that this function can be considered as the bounded hamiltonian of a quantum system,
thereupon obtaining self-consistency with number theory, if and only if, the cardinal of the factorization ensemble coincides with the dimension of the corresponding Hilbert space. This fact links directly quantum mechanics with number theory. Moreover, given the relation between the primes and the \( \zeta(s) \) function zeroes, it could be also related to the problem of implementing Polya and Hilbert conjecture for the solution of the Riemann’s hypothesis (see e.g. [2] and more recently the proposal in [3], but note that their formulation does not allow to propose a physically realizable system). Here we concentrate in the physical realization of the quantum device supporting Eq. [3].

**Formulation of the quantum conditions.** For the primes in \( \mathcal{F}(j) \), one gets \( q < q_m \) for some maximum coordinate. Then, we are allowed to use quantum transformation theory to build the finite and normalizable quantum amplitude of probability \( \Psi(q) \) for the \( q \)-numbers,

\[
\Psi'' + q^2 \Psi = E \Psi,
\]

The constraints are \( \Psi(\sqrt{E}) = 0 \), \( \Psi(q_m) = 0 \). The solutions are stationary waves,

\[
\Psi(q) = q e^{-i \frac{q^2}{2}} [F(\alpha, \frac{3}{2}, i q^2) + D(E) \cdot U(\alpha, \frac{3}{2}, i q^2)]
\]

Here, \( F(a, b, z) \) and \( U(a, b, z) \) denote the two linearly independent confluent hypergeometric functions, \( \alpha = -\frac{D}{4} + \frac{3}{2} \), and \( D(E) \) is a suitable complex constant required to satisfy the constraints. The uniqueness of the solution of the Sturm-Liouville problem implies the quantization of \( E \):

\[
F(\alpha, \frac{3}{2}, i q_m^2) U(\alpha, \frac{3}{2}, i E) U(\alpha, \frac{3}{2}, i q_m^2) = 1,
\]

**The spectrum of energies.** If \( E = O(1) \), i.e., for factors close to \( \sqrt{N} \), one can solve Eq. [6] as a series \( E = 1 + \varepsilon(q_m) + O(\varepsilon^2) \). After a straightforward, albeit long, calculation we get

\[
\varepsilon(q_m) \approx \frac{1}{\log q_m} \{ \tan \phi_0 + \sin \phi_m \sec \phi_0 \},
\]

where \( \phi_m = q_m^2 - q_0^2 - \log(q_m/q_0) - \phi_0, \phi_0 \approx 1.11966 \), is a universal constant and \( q_0 \) is an arbitrary phase that can be added to the solution since it is a periodic function of the coordinate bound \( q_m \). Indeed this is an equation that relates \( E \) with the integers because by construction \( q_m \) should be calculated for some prime in the ensemble. To see this, assume we can (classically) determine that \( x \) is much larger than some known bound \( B(G) \) and that, for other numbers \( N_k \) in \( \mathcal{F}(j) \), the bound \( B_k \) is a prime in the vicinity of \( B(G) \). Then

\[
\pi(B_k) = \pi(B(G)) - k.
\]

Therefore, we should prepare the state \( \Psi(q) \) with the boundary condition at \( q_m(k) = q \pi(B_k) \), for \( k \) integer. Now, since \( B(G) \ll x = O(\sqrt{N}) \), for some constant \( G \), consider the ”Ansatz”

\[
q_0 = \frac{N^{1/6}}{(\log \sqrt{N})^G}.
\]

It allows to compute \( q_m(k) \), using the prime number theorem, as a series in the small parameter \( \lambda = q_0^2/\sqrt{N} \), \( q_m(k) = q_0 + \frac{2}{\pi} \lambda k + O(\lambda^2 k^2) \), which means that \( q_0 \) is essentially the size of the simulator. This size should indeed be taken as an exact zero of the function in Eq. [3] for \( E = 1 \). Finally we obtain for the energies

\[
E_k(G) \approx 1 + \frac{k}{k_m \log q_0} + O(k/k_m)^2,
\]

where \( k_m = \frac{3}{2} \pi (\log \sqrt{N})^G \), is the period of Eq. [7]. It must also be the number of stationary states of the simulator for some gauge \( G \); it scales only logarithmically with the number \( N \). Eq. [10] also predicts the kind of linear integer \( k \) dependence observed in Fig. 1. Moreover, given the arbitrariness of the gauge, a kernel density estimation average can be determined. Then, the predicted spectrum from our quantum mechanical solution Eq. [10], that corresponds to the distribution of the primes in \( \mathcal{F}(j) \) (for our example, \( j = 10000 \)), can be compared versus de actual one. To this aim, we have represented the density plots for the theoretically predicted pairs \( (E_k, x_k) \), and that obtained from counting the primes in \( \mathcal{F}(10000) \) in Figs. 2 and 3 respectively. The probability for a prime to be a factor is highest in the red area and lowest in the white areas. There exists a pretty reasonable concordance between both. Thus, quantum mechanics obtains in \( \mathcal{F}(j) \) the apparently unpredictable jumps in the distribution of the primes, a feature that confirms again the relation between physics and number theory. This result is complementary to the prediction of the regular behavior of \( \pi(x) \) in [3]. Recall that, in order to calculate the results in Fig. 2 we computed the energies for gauges corresponding to the first ten zeroes of the wave function (other zeroes provide energies greater than that required for the plot). To mimic the output of the simulator we ought to make a Montecarlo calculation replacing, in Eq. [10], \( \sqrt{N} \) by \( \sqrt{N} \varepsilon = (\sqrt{N} - \log \sqrt{N}, \sqrt{N} + \log \sqrt{N}) \), i.e.,
other values in $\mathcal{F}(j)$ that contribute with slightly different energy levels $E_k(G')$. We then calculated $x_k(E_k(G'))$ after the definition in Eq. (2). Finally we plotted, using the kernel density estimation average from these values, the distribution of $O(\log \sqrt{N})^3$ random points with this metric. Notice that since $E_k = \mathcal{F}(\pi(x_k), \pi(N_k/x_k))$, we needed Riemann’s Fourier expansion of $\pi(x)$ in terms of the $\zeta(s)$ function zeroes. To elaborate the result of Fig. 2 we used a truncated series of 300 zeros to approximate $\pi(x)$.

Then, identifying $\varrho$ as a polar radial coordinate, we get very approximately, for $\varrho \gg (\hbar/2^{1/2}M\omega_c)^{1/2}$
\begin{equation}
- \frac{\hbar^2}{2M} \frac{1}{\varrho} \frac{\partial}{\partial \varrho} \varrho \frac{\partial \psi}{\partial \varrho} - \frac{M\omega_c^2}{4} \varrho^2 \psi \simeq E' \psi. \tag{12}
\end{equation}
This is readily interpreted as the Schrödinger equation satisfied by a $l_z = 0$ state with axial symmetry. The classical limit must then correspond to a system which is confined, both radially and axially, in interaction with the potential energy $-\frac{M\omega_c^2}{4} \varrho^2$ which could be identified as an electrostatic field. The form of this potential directly leads to identify Eq. (12) with the hamiltonian constraint corresponding to the physics of a Penning trap [9]. In this system, the charged particles remain trapped radially by a magnetic field and axially by a quadrupolar electrostatic field which means that the particles must have also spin. Moreover, compatibility of the zero axial component of the angular momentum suggests that the system can be, for instance, a $p$-wave or a $s$-wave of two electrons. These features might correspond to two different kind of Bell states made by two electrons with mass $m_e = M/2$:
\[
|p_\pm> = 1/\sqrt{2}(|\uparrow\uparrow> \pm |\downarrow\downarrow>)
\]
or
\[
|s_\pm> = 1/\sqrt{2}(|\uparrow\downarrow> \pm |\downarrow\uparrow>)
\]
(recall that, for a $p$-wave, $E' \rightarrow E' + e\hbar/m_e c B$). Moreover, notice that in Eq. (12) no electrostatic interaction appears and therefore the Coulomb energy must be added as a constant $e^2/x_0$, where $x_0/2$ are the coordinates of the diametrically opposed equilibrium positions for the two electrons. The coordinate wave function is, thus, antisymmetric, which leads to only spin symmetric $p_+$ or $s_+$ possible configurations. A way to experimentally build these kind of equilibrium Bell states was proposed in [10] using, first, a rotational barrier to spatially separate the electrons and then, in order to achieve entanglement, a resonant oscillating electric field is applied to drive the axial degree of freedom. Once the Bell state is achieved, to get the interaction back to that in Eq. (12), the rotational barrier must be adiabatically reduced to zero in time scale larger than the inverse of the Rabi frequency of the drive. This procedure transfers a spatial antisymmetric configuration to the quantum state compatible with $l_z = 0$.

The two constant cyclotron frequencies are given by $\omega_c = \pm e/\hbar c B$, for parallel $(\pm)$ and antiparallel $(\mp)$ spins. In a Penning trap, the classical motion is fully described by three frequencies namely, the cyclotron frequency $\omega_c$, the electrical oscillator $\omega_z$ and the magnetron frequency for the radially confined motion $\omega_m$. Thus Eq. (12) normally represents the quantization of the magnetron motion. Moreover, it holds that, for the trap to be operative, $\omega_c \gg \omega_z \gg \omega_m$, $\omega_m \simeq \omega_z^2/2\omega_e$, with $\omega_e$ slightly smaller than the cyclotron frequency and $\omega_e \geq \sqrt{2}\omega_z$. Then, the $z$-motion decouples from the radial coordinate magnetron motion resulting in a simple harmonic oscillator

\[
\text{FIG. 2. Density plot for the distribution of values (}E_k, x_k\text{) calculated quantum mechanically for the simulator of }\mathcal{F}(10000). \text{ Red areas correspond to the highest probability and white to the lowest.}
\]

\[
\text{FIG. 3. Actual density plot for the distribution of values (}E_k, x_k\text{) for the primes in }\mathcal{F}(10000). \text{ The scale is the same than in the previous figure. Again, red areas correspond to the highest probability and white to the lowest.}
\]

\textbf{Physical realization of the quantum state.} The simulator is a physical system. To see a possible experimental set up, first in Eq. (4) we make the substitutions
\[
q \rightarrow \left(\frac{M\omega_c}{2^{1/2}\hbar}\right)^{1/2} \varrho, \ E \rightarrow -2\sqrt{2} \frac{E'}{\hbar\omega_z}, \\
\Psi(q) \rightarrow \psi(\varrho)\varrho^{1/2}.
\tag{11}
\]

Then, identifying $\varrho$ as a polar radial coordinate, we get

\[
- \frac{\hbar^2}{2M} \frac{1}{\varrho} \frac{\partial}{\partial \varrho} \varrho \frac{\partial \psi}{\partial \varrho} - \frac{M\omega_c^2}{4} \varrho^2 \psi \simeq E' \psi. \tag{12}
\]
of frequency $\omega_z$. This experimental set up confines the charges in a saddle point region $\varrho, z$, where $\varrho < \varrho_m$, corresponding to the size of the ring electrode. The quantized energy of the magnetron motion is exactly decoupled from the cyclotron motion [3]. It is given by,

$$E' = -\hbar \omega_m (k + 1/2) \Leftrightarrow E \approx \sqrt{2} \frac{\omega_z}{\omega_c} (k + 1/2),$$

which corresponds to the linear dependence calculated for the isolated inverted harmonic oscillator, Eq. (10), if and only if we impose

$$\omega_z/\omega'_c = 1/\log q_\varrho \cdot \frac{\pi \sqrt{2}}{k_m}. \quad (14)$$

On the other hand, the size of the electrostatic quadrupole potential restricts the trajectories of the electrons to the saddle point area. Then $\psi(q)$ will be non zero if $q < q_m$ and $\psi(q) = 0$ otherwise. It reads (recall $M = 2m_e$ and that $q_m \simeq q_\varrho$)

$$q_m \simeq \left( \frac{\hbar}{2\sqrt{2m_e \omega_z}} \right)^{1/2} q_\varrho \Leftrightarrow \omega_z = \sqrt{2} \frac{\hbar q_\varrho^2}{2m_e q_m^2}. \quad (15)$$

Now from Eq. (14), Eq. (9) taken into account, one finally gets, for the Number that a technologically achievable trap is able to simulate,

$$\sqrt{N} \approx \frac{2q_\varrho^3}{3} \left[ \frac{q_\varrho}{2\log q_\varrho} \frac{m_e^2 B}{\hbar c/2e} \right], \quad (16)$$

recall that the term inside the square brackets is the quantum of the magnetic flux through the trap, $m$, implying that only discrete energy levels are permitted (Landau levels). Therefore the number of operative qubits of the simulator is exponentially large $2^n$. This physical set up is akin to the proposal in [11] to experimentally determine Riemann’s zeroes if Polya and Hilbert conjecture applies.

For electron traps with $q_m \sim 3$ mm, typical electrostatic fields yield to $q_\varrho \lesssim 10^2$ while $(\omega_z/\omega_c) \sim 10^3$, then numbers up to $N \lesssim 10^{20}$ can be factorized with the quantum simulator. Measuring the magnetron frequencies $|E'|/\hbar$, gives $E = 2\sqrt{2}(|E' - \hbar e/mcB|)/\hbar \omega_z$ ($L = 0, 1$ for the $s$-wave and $p$-wave, respectively). The only meaningful values being those with $E > 1$.

The simulator operates as follows: take, e.g., $q_\varrho = 2.82765$, the first zero of the wave function for $E = 1$, then Eq. (15) fixes $\omega_z$ and, in order to code the number we wanted to factorize in the simulator, the magnetic field frequency is fine tuned with the help of Eq. (16). Then, upon selecting new zeroes of the wave function $q_\varrho$, and re-scaling the field frequencies of the trap accordingly, other sets of energies of the simulator could be measured; this procedure, depending on the number of measurements, typically $O(\log \sqrt{N})$, would yield to a detailed probabilistic density pattern in a neighbourhood of each measured energy where the more probable values of $E_k$ will cumulate. It will result in a probabilistic quantum sieve for the more likely $x(E)$ factors in the ensemble. Given that linear jumps in $E$ ought to correspond to exponentially large ones in $x$, the simulator yields to an exponential speed up to find the factors, though recall that, to finally exactly calculate $x$ and $y$, a classical sieve would still be required provided the probability input for primes $O(\sqrt{N})$.

Discussion. As it is always the case in quantum mechanical calculations a solution can only be provided in a statistical way. In this sense, the theory provides the most probable prime factors of $N$. On the other hand, independently of the physical realization of the simulator, one can always think the result in Eq. (10) as a new probabilistic quantum enhanced factorization algorithm where the number $\sqrt{N}$ is considered as a parameter. To provide a probability density estimation for the primes that most likely factorize $N$, the physically realizable simulator only requires an amount of $O(\log \sqrt{N}) \log q_\varrho$ energy measurements and, in this sense, it provides a polynomial probabilistic quantum sieve. We finally introduced a physical realization of the simulator consisting in preparing a Bell state for two electrons in a Penning trap. Thus, in the end, the reason of the factoring exponential speedup of the simulator should be the coupling of the entangled state with the quantized flux of the magnetic field. Recall that, apart from the $p_+$ and $s_+$ waves, other different symmetric spin states with more than two electrons are compatible with the constraint $l_z = 0$ in the Penning trap and that it will likely allow to experimentally scaling the simulator even for much larger $N$’s.

This work has been partially supported by Comunidad Autónoma de Madrid, project Quantum Information Technologies Madrid, QUITEMAD+ S2013/ICE-2801, and by project CVQuCo, Ministerio de Economía 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] L.M.K Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, I. L. Chuang (2001)”Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance” Nature 414-20,27 pp 884 – 887.
[5] Latorre, J.I and Sierra, G. (2014) “Quantum Computa-
tion of Prime Number Functions”, Quantum Information and Computation, Vol. 14 Issue 7 and 8 Pages 577-588
[6] Rosales, J.L. and Martin, V. (2016) "Quantum Simulation of the Factorization Problem", Phys. Rev. Lett. 117, 200502
[7] D. Schumayer and D.A.W. Hutchinson, Physics of the Riemann hypothesis, Rev. Mod. Phys. 83, 307 (2011).
[8] C. M. Bender, D. C. Brody, M. P. Müller, (2017), "Hamiltonian for the zeros of the Riemann zeta function", Phys. Rev. Lett. 118, 130201

[9] 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.
[10] Lamata, L., Porras, Cirac, J.I, Goldman, J and Gabrielse, G. (2010), "Towards electron-electron entanglement in Penning traps", Phy. Rev. A 81, 022301.
[11] G. Sierra and P. K. Townsend (2008), "Landau Levels and Riemann Zeros", Phys. Rev. Lett. 101, 110201