Identifying primes from entanglement dynamics

A. L. M. Southier,1 L. F. Santos,2 P. H. Souto Ribeiro,3 and A. D. Ribeiro1

1Departamento de Física, Universidade Federal do Paraná, 81531-990, Curitiba, PR, Brazil
2Department of Physics, University of Connecticut, Storrs, CT, USA
3Departamento de Física, Universidade Federal de Santa Catarina, 88040-900, Florianópolis, SC, Brazil

Factorization is the most fundamental way to determine if a number n is prime or composite. Yet, this approach becomes impracticable when considering large values of n, a difficulty that is exploited by cryptographic protocols. We propose an alternative method to decide the primality of a natural number, that is based on the analysis of the evolution of the linear entanglement entropy. Specifically, we show that a singular behavior in the amplitudes of the Fourier series of this entropy is associated with prime numbers. We also discuss how this idea could be experimentally implemented and examine possible connections between our results and the zeros of the Riemann zeta function.

Prime numbers have captured the attention of researchers for centuries. In pure mathematics, given the prominent role of primes in factorizing a positive integer n, much effort has been made to unravel patterns in their distribution over the set of natural numbers \( \mathbb{N} \). Remarkable results in this direction involve the connection of the Riemann zeta function \( \zeta(s) \), which is a complex variable, defined as \( \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \). The complete knowledge of \( \pi(n) \) would imply being able to determine the position of each prime factor of a huge n, which would require the implementation of Shor’s algorithm in a quantum computer.

Another fascinating result involving primes is their connection with the zeros of the Riemann zeta function, where s = \( \frac{1}{2} \) and the Gamma function \( \Gamma(1-s) \) encodes the distribution of primes less than or equal to n. The complete knowledge of \( \pi(n) \) would imply being able to determine the position of each prime number p, since jumps of this function expose their presence. However, achieving the counting function with satisfactory accuracy for large values of n has been shown to be practically impossible. In applied mathematics, this lack of knowledge is exploited for cryptographic protocols, such as the RSA (Rivest-Shamir-Adleman) algorithm. To break the RSA protocol, one needs to find the prime factors of a huge n, which would require the implementation of Shor’s algorithm in a quantum computer.

The summation and the product above converge when the real part of the variable s satisfies \( \Re[s] > 1 \). The first equality in Eq. (1) is due to Euler and makes evident the relation between \( \pi(n) \) and \( \zeta(s) \). In 1859 [4], Riemann achieved the expression shown on the right side of Eq. (1), which involves a line integral along a particular path \( \gamma \) and the Gamma function \( \Gamma(1-s) = \int_{0}^{\infty} x^{s-1}e^{-x}dx \). The expression is analytic for all values of s, except for a simple pole at s = 1. In the region \( \Re[s] > 1 \), the term with the integral recovers the other two expressions in Eq. (1), so one considers it as their analytic continuation. Using these ideas, Riemann [4] demonstrated how the complex zeros \( s_0 \) of \( \zeta(s) \) encode the distribution of \( \pi(n) \). Specifically, he showed that a certain convergent series, running over all \( s_0 \), recovers the function \( \pi(n) \). But for large values of n, the number of zeros required to accurately get the counting function is so large that the use of the series to identify \( p \) becomes intractable. This sophisticated connection between \( \zeta(s) \) and primes is but one of the impressive results of Ref. [1]. Arguments in that work also gave origin to the Riemann hypothesis, which conjectures that \( \Re[s_0] = \frac{1}{2} \) for all nontrivial zeros of \( \zeta(s) \).

Identifying primes from entanglement dynamics...
of the linear entanglement entropy encodes prime and semiprime numbers. Specifically, we demonstrate that the Fourier modes \( c_n \) of this evolving function have amplitudes that present a singular behavior when \( n \) corresponds to a prime, and we find curves \( c'_n \) for the location of families \( f \) of semprimes. This is shown for a system of two coupled harmonic oscillators and a system of two coupled spins. We discuss a possible experimental realization of this idea and speculate on how to link \( c_n \) and the counting function \( \pi(n) \).

Entanglement dynamics.— We consider a system consisting of two interacting parts, \( A \) and \( B \), to which we assign distinct Hilbert spaces, \( \mathcal{H}_A \) and \( \mathcal{H}_B \), respectively. The system is isolated and prepared in a pure state, \( \rho(0) = |\Psi(0)\rangle \langle \Psi(0)| \), which evolves according to the total Hamiltonian

\[
H = H_A \otimes 1_B + 1_A \otimes H_B + \lambda H_A \otimes H_B,
\]

where \( \lambda \) is the coupling strength between the two subsystems. The linear entanglement entropy,

\[
S_L(t) = 1 - \text{Tr} \left[ \rho_A^2(t) \right],
\]

where \( \rho_A(t) = \text{Tr}_B[\rho(t)] \) is the reduced density matrix of system \( A \), measures the bipartite entanglement in time between \( A \) and \( B \). When \( \rho(t) \) is separable, \( S_L(t) = 0 \), otherwise \( 0 < S_L(t) < 1 \).

Coupled oscillators.— The first Hamiltonian that we consider describes two coupled harmonic oscillators, where \( H_A \) is the Hamiltonian for part \( A \) with eigenvalues \( \hbar \omega_0(n_A + \frac{1}{2}) \) and eigenstates \( |n_A\rangle \), and equivalently for part \( B \). The initial state is the product of two canonical coherent states \( |\alpha_A \alpha_B\rangle \equiv e^{-u^2/2} \sum_{n_A,n_B=0}^{\infty} \frac{\alpha_A^{n_A}}{\sqrt{n_A!}} \frac{\alpha_B^{n_B}}{\sqrt{n_B!}} |n_A n_B\rangle \),

where we chose \( |\alpha_A|^2 = |\alpha_B|^2 = \frac{\hbar \omega_0^2}{2} \). Defining \( \omega \equiv \hbar \omega_0^2 \),

\[
S_L^{osc}(t) = 1 - e^{-2u^2} \sum_{j,k,l,m} \frac{u^{j+k+l+m}}{j! k! l! m!} e^{-i\omega t(j-k)(l-m)}. \tag{4}
\]

The sum above runs from 0 to \( \infty \) for all indexes. Since the entropy in Eq. (4) is periodic in time, with period \( T = 2\pi/\omega \), we use the Fourier series and arrive at

\[
S_L^{osc}(t) = c_0(u) - \sum_{n=1}^\infty c_n(u) \cos(n\omega t), \tag{5}
\]

where the coefficients \( c_n(u) \) are given by

\[
c_n(u) = 4 e^{-2u} \sum_{k,m,j>l > m} \frac{u^{j+k+l+m}}{j! k! l! m!} \delta_n^{(j-k)(l-m)}, \tag{6}
\]

representing the amplitude of the mode with frequency \( n\omega \). In Eq. (6), the Kronecker delta function, \( \delta_a^b \) for integers \( a \) and \( b \), prompts the analysis of how \( n \) decomposes as a product of two integers. We introduce the set \( \Lambda_n \) composed of all distinct positive divisors of \( n \) and note that the non-null terms in Eq. (6) are those for which \((j-k) \) and \((l-m)\) belong to \( \Lambda_n \) and their product equals \( n \). Therefore,

\[
c_n(u) = 4 e^{-2u} \sum_{\mu \in \Lambda_n} I_\mu(u) I_{\frac{n}{\mu}}(u), \tag{7}
\]

where \( I_\mu(u) \equiv \sum_{k=0}^{\infty} [k!(\chi+k)!]^{-1} (\frac{\mu}{2})^{2k+\chi} \) is the modified Bessel function of the first kind. As we show next, \( c_n(u) \) is very sensitive to the primality of \( n \).

Identifying primes.— To show that the entanglement dynamics quantified by \( S_L^{osc}(t) \) is a prime identifier, we first assume that \( n \) is prime, so that \( \Lambda_n = \{1,n\} \) and Eq. (7) yields \( c_n(u) = c^{(p)}_n(u) \), where

\[
c^{(p)}_n(u) = 4 e^{-2u} I_1(u) I_n(u). \tag{8}
\]

In contrast, when \( n \) is as a composite number, \( \Lambda_n \) necessarily consists of 1, \( n \), and, at least, one more integer. By defining the set \( \Lambda'_n = \Lambda_n - \{1,n\} \), Eq. (7) becomes

\[
c_n(u) = c^{(p)}_n(u) + 4 e^{-2u} \sum_{\mu \in \Lambda'_n} I_\mu(u) I_{\frac{n}{\mu}}(u) \geq c^{(p)}_n(u), \tag{9}
\]

which holds only for \( n > 1 \).

Inequality (9) is a main result of this work. It shows that the coefficients \( c_n(u) \) coincides with \( c^{(p)}_n(u) \) in Eq. (8) if, and only if, \( n \) is prime, while for composite numbers, the amplitudes are strictly lower bounded by \( c^{(p)}_n(u) \). This means that if we have a way to determine the values of \( c_n(u) \), other than through the construction of \( \Lambda_n \), the application of Eq. (9) can reveal the primality of \( n \). Indeed, \( c_n(u) \) can be evaluated theoretically via Eq. (4) and possibly experimentally.

In Fig. (a) we mark the values of \( c_n(u) \) with blue dots. For each \( n \) identified as a prime, the dots are encircled with a black circle. All values of \( c_n(u) \) corresponding to primes coincide with the red dotted line that represents the lower bound \( c^{(p)}_n(u) \) and can, therefore, be clearly distinguished. In Fig. (a), we show results for \( u = 1 \), but \( c_n(1) \) becomes too small when \( n \) is large, so in Fig. (b), we use \( u = 10^3 \) and larger values of \( n \).

Semiprimes.— Figure (b) also reveals the square-free semiprimes, including the integer 2, which we denote by family \( f_2 \). For these numbers, \( \Lambda_n = \{1,2,P_n,n\} \), where \( P_n = n/2 \neq 2 \) is a prime, and \( c_n(u) = c^{(2)}_n(u) \), where

\[
c^{(2)}_n(u) \equiv 4 e^{-2u} \left[ I_1(u) I_n(u) + I_2(u) I_2(u) \right]. \tag{10}
\]

For a composite \( n \) that presents the divisors: 1, 2, \( n/2 \), \( n \), and at least one more integer,

\[
c^{(2)}_n(u) \equiv c^{(2)}_n(u) + 4 e^{-2u} \sum_{\mu \in \Lambda^{(2)}_n} I_\mu(u) I_{\frac{n}{\mu}}(u) > c^{(2)}_n(u),
\]

where \( \Lambda^{(2)}_n \) composed of all distinct positive divisors of \( n \) which are less than or equal to \( \sqrt{n/2} \).
where \( \Lambda_n^{(2)} = \Lambda_n - \{1, 2, n/2, n\} \). The semiprimes of family \( f_2 \) are identified with black squares in Fig. 1 and they all fall on the curve \( c_n^{(l)}(u) \), indicated with a green line. This line consists of a lower bound for any integer composed by 2, except for 2, 2^2, and 2^3.

It is straightforward to extend the analysis above to any other family of semiprimes. The particular case of the square-free semiprimes containing the number 3, denoted by \( f_3 \), is shown in Fig. 1. The components of family \( f_3 \) are marked with black triangles and they are exactly located over the cyan curve \( c_n^{(l)}(u) \).

**Interacting spins.** — Analogously to the system of coupled harmonic oscillators, we now show that two interacting spins with a large quantum number \( S \) is another physical system that can be used to identify primes. In the Hamiltonian of Eq. (2), we assume that \( H_A = \hbar \omega_0 S_A^z \), where \( S_A^z \) is the \( z \)-component of the spin operator of part \( A \) and \( S_A^z|m_A\rangle = m_A|m_A\rangle \), and equivalently for part \( B \). The initial state is the product of spin coherent states \( |s_{A,B}\rangle \), where

\[
|s_{A,B}\rangle \equiv N_s \sum_{n_A, n_B = 0}^{2S} \frac{s_{A,B}^{n_A, n_B}}{\sqrt{(2S)! n_A! n_B!}} |n_A - S, n_B - S\rangle,
\]

where \( N_s = (1 + u)^{-2S} \) and we chose \( |s_A|^2 = |s_B|^2 = u \).

The evolving linear entanglement entropy \( S_{L}^{\text{spin}}(t) \) becomes

\[
S_{L}^{\text{spin}}(t) = 1 - \sum_{j,k,l,m=0}^{2S} \xi_{j,k,l,m} u^{j+k+l+m} e^{-i\omega_t(j-k)(l-m)},
\]

where \( \xi_{j,k,l,m} \equiv \left( \begin{array}{c} 2S \end{array} \right)^{\left( \begin{array}{c} j \end{array} \right)} \left( \begin{array}{c} 2S \end{array} \right)^{\left( \begin{array}{c} k \end{array} \right)} (1+u)^{-8S} \). The Fourier series of Eq. (11) has the same structure as Eq. (5), but with the coefficients

\[
\tilde{c}_n(u) = 4 \sum_{k,m=0}^{2S-1} \sum_{j,k,l,m} \xi_{j,k,l,m} u^{j+k+l+m} \delta_{j-k}(l-m).
\]

The nonvanishing terms in the equation above are again those for which \( \mu \equiv (j-k) \) and \( \nu \equiv (l-m) \) belong to the set \( \Lambda_n \) of divisors of \( n \). However, this system is bounded, so the upper limits of the above summations add new constraints to \( \mu \) and \( \nu \). Given a value for \( k \) and \( m \), we have that \( \mu \in I_k \equiv [1, 2S-k] \) and \( \nu \in I_m \equiv [1, 2S-m] \). In addition, since \( \delta_{j-k} \) implies that \( \nu = n/\mu \), we also get that \( \mu \in I_{m,n} \equiv \left[ \frac{m}{2S-m}, n \right] \). Therefore,

\[
\tilde{c}_n(u) = 4 \sum_{k,m=0}^{2S-1} \sum_{\mu} \xi u^{2k+2m+\mu+n/\mu},
\]

where \( \xi = \xi_{k+\mu,k,m} \). The set of divisors \( \Lambda_n^{(k,m)} \) is the set of divisors of \( n \) that satisfies all constraints commented above,

\[
\tilde{\Lambda}_n^{(k,m)} = \Lambda_n \cap I_k \cap I_{m,n}.
\]

Contrary to \( S_{L}^{\text{osc}}(t) \) in Eq. (5), there is a finite number of Fourier modes in \( S_{L}^{\text{spin}}(t) \) due to the finite Hilbert space for the spin system. For \( n > 4S^2 \), we have that \( I_k \cap I_{m,n} = \emptyset \) for any value of \( k \) and \( m \), so \( \tilde{\Lambda}_n^{(k,m)} = \emptyset \) and \( \tilde{c}_n(u) = 0 \). In what follows, to assess the primality of \( n \), we conveniently divide the interval \( 1 < n < 4S^2 \) in two regions of interest, region I \( (1 < n < 2S) \) and region II \( (2S < n < 4S) \). In the complementary range \( 4S < n < 4S^2 \), one cannot find a behavior that distinguishes primes from composite numbers. There, even though all amplitudes of the Fourier modes for a prime \( n \) vanish, the same can also happen to some composite numbers.

Region I \( (1 < n < 2S) \) reveals that \( 1 \in \tilde{\Lambda}_n^{(k,m)} \) for all values of \( k \) and \( 0 < m < 2S-n \), while \( n \notin \tilde{\Lambda}_n^{(k,m)} \) for all values of \( m \) and \( 0 < k < 2S-n \). Applying these results to Eq. (12), we find that, for \( n \) prime, \( \tilde{c}_n(u) = \tilde{c}^{(p)}_{n,l}(u) \), where

\[
\tilde{c}^{(p)}_{n,l}(u) = 8 (1+u)^{-8S} G_1(u) G_n(u),
\]
with $G_{\chi}(w) \equiv \sum_{k=0}^{2S-\chi} \binom{2S}{k} (2^k \chi) w^{2k+\chi}$. On the other hand, for a composite number $n > 1$ inside region I, we have that $\tilde{c}_n(u) = \tilde{c}^{(p)}_n(u) + \tilde{d}_{n,I}(u)$, where

$$d_{n,I}(u) = 4 \sum_{k,m=0} \sum_{\mu \in \Lambda^{(k,m)}_{n,u}} \xi u^{2k+2m+\mu+n/\mu}$$

and $\Lambda^{(k,m)}_{n,u} \equiv \Lambda_n \cap \mathcal{I}_k \cap \mathcal{I}_{m,n}$, where $\Lambda_n$ was defined above Eq. (17). One can show that at least for $k = m = 0$, there is a positive non-null term in Eq. (15). Therefore, for a composite number, we necessarily have $\tilde{c}_n(u) > \tilde{c}^{(p)}_n(u)$ and this inequality can be employed in the search for prime numbers in region I.

Region II ($2S < n \leq 4S$): In this case, prime modes are not included in the Fourier series of Eq. (11). Indeed, for a prime number $n$, we now have that $1 \not\in \mathcal{I}_{m,n}$ and $n \not\in \mathcal{I}_k$, which implies that $\Lambda^{(k,m)}_{n} = \emptyset$ and $\tilde{c}_n(u) = 0$. For a composite $n$ in the same interval, similarly to region I, there is at least one integer in $\Lambda_n$, in addition to 1 and $n$, so that $\tilde{c}_n(u) > 0$. So we can distinguish primes from composite numbers by checking if $\tilde{c}_n(u) = 0$ or $\tilde{c}_n(u) \neq 0$.

**Experimental proposal.** — The Hamiltonian for the two coupled harmonic oscillators studied above also describes the interaction between two optical fields via a Kerr nonlinear medium [30, 31]. In Fig. 2, we show the sketch of an experimental setup for implementing this optical system. A laser beam of frequency $\omega_0$ and linear polarization at 45° is sent to a polarizing beam splitter (PBS). The vertically polarized ($\downarrow$) component goes directly to the homodyne detection scheme [32], shown in the lower right corner of the figure, to act as the local field. The horizontally polarized ($\leftrightarrow$) component passes through a half wave plate (HWP), which rotates the polarization to 45°, and enters an unbalanced Mach-Zehnder interferometer, identified in Fig. 2 with dashed lines. In the interferometer, after the PBS, the $\uparrow$ component beam propagates through the short path, and the $\leftrightarrow$ one goes through the long course. The path difference is longer than the coherence length, so that the recombined $\leftrightarrow$ and $\uparrow$ beams at the interferometer output PBS are separable and no longer result in a pure mode with linear diagonal polarization. Next, these two beams are injected in the nonlinear Kerr medium (KM) of length $L$ and Kerr optical nonlinearity $\chi^{(3)}$. During the propagation time inside the KM, each beam will experience a modified index of refraction due to the action of the other beam. This is how the coupling between the oscillators is physically implemented. By varying the length $L$, one changes the interaction time $t$. After passing KM, the $\leftrightarrow$ and $\uparrow$ beams are split again. To identify the prime numbers, we measure one of the beams and ignore the other, which is equivalent to performing the trace over one of the interfering systems. We can analyze any of the two beams because of the interaction symmetry. In Fig. 2, we choose the $\uparrow$ beam, which goes to the homodyne detector, where quantum state tomography is performed to reconstruct the density matrix $\rho_A$. With the reduced density matrix, we calculate the linear entanglement entropy. After several experimental realizations spanning the needed values of $t$, curves like those in Fig. 1 can be generated.

**Conclusion.** — This paper shows that by analyzing the bipartite entanglement in time, one can identify prime and semiprime numbers in $\mathbb{N}$. The main ingredient is a Hamiltonian composed of two parts, $A$ and $B$, with equidistant energy levels for $H_A$ and $H_B$. We discussed how this idea could be implemented taking advantage of an existing experimental setup.

Our work resonates with the Hilbert–Pólya conjecture in the sense of proposing a physically measurable quantity to determine prime numbers. We speculate that there may be a way to connect our results with $\zeta(s)$. In fact, by defining $A(n, u) \equiv c_n(u) - c^{(p)}_n(u)$ for a fixed $u$, the task of counting primes along $\mathbb{N}$ is equivalent to counting the zeros of $A(n, u)$. This alternative method to build $\pi(n)$ could be used to study the zeros of $\zeta(s)$ by means, for example, of a hypothetical inversion of the Riemann series that connects $\zeta(s)$ with $\pi(n)$, shedding new light on the Riemann hypothesis.

Our last remark concerns the semiclassical approaches originated from the ideas of Berry and Keating [8]. The semiclassical version of the linear entanglement entropy was addressed in [33, 54] for the same two physical systems treated here. In those papers, entanglement is reproduced by summing over sets of classical trajectories determined by the solutions of a given transcendental equation. The purely quantum formalism presented here encourages the re-examination of those works aiming at connecting those solutions with the distribution of primes.

**ACKNOWLEDGEMENTS**

This study was financed by the Brazilian agencies: Fundação de Amparo à Pesquisa do Estado de Santa Catarina (FAPESC – DOI 50110005667), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES – DOI 50110002322), Conselho Nacional de


H. M. Edwards, *Riemann’s zeta function* (Dover, New York, 1988)

N. Koblitz, *The path of integration* (Springer-Verlag, New York, 1991)


Ran He, Ming-Zhong Ai, Jin-Ming Cui, Yun-Feng Huang, Yong-Jian Han, Chuan-Feng Li, Tao Tu, C. E. Cressfield, G. Sierra, and Guang-Can Guo, Identifying the Riemann zeros by periodically driving a single qubit, Phys. Rev. A 101, 043402 (2020)


