Primes go Quantum:

there is entanglement in the primes

Germán Sierra
In collaboration with José Ignacio Latorre
Madrid-Barcelona-Singapore

Workshop:
Entanglement Entropy in Quantum Many-Body Systems
King's Collegue and City University, London, 2-4 June 2014
Plan

• A primer of prime numbers
• Primes and Physics
• Prime state
• Entanglement of the Prime state
• Conclusions

Based on arXiv: 1302.6245 and arXiv:1403.4765
Prime counting function

\[ \pi(x) : \text{number of primes } p \text{ less than or equal to } x \]

\[ \pi(100) = 25 \]


Asymptotic behaviour: Gauss law

\[ \pi(x) \approx Li(x) \approx \frac{x}{\ln x} \]

\[ x \rightarrow \infty \]

Average behaviour
Prime Number Theorem (PNT)  
- Hadamard (1896)  
- de la Vallee-Poussin

Density of primes:  
\[
\frac{d\pi(x)}{dx} \approx \frac{1}{\ln x}
\]

Largest known value  
\[\pi(10^{24}) = 18\,435\,599\,767\,349\,200\,867\,886 \approx 1.8 \times 10^{22}\]  
Platt (2012)

\[Li(10^{24}) - \pi(10^{24}) \approx 1.7 \times 10^{10}\]

The prime number function must oscillate around the Li(x) infinitely many times  
(Littlewood)

A first change of sign is expected for occur below the Skewes number
The fluctuations of around are expected to be bounded by

This statement is equivalent to the Riemann hypothesis (RH)
The zeta function and the Riemann hypothesis

Rosetta stone for Maths

\[ \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{Re} \ s > 1 \]

\[ \zeta(s) = \prod_{p=2,3,5,\ldots} \frac{1}{1-p^{-s}}, \text{Re} \ s > 1 \]

\[ \zeta(s) = \frac{\pi^{s/2}}{2(s-1)\Gamma(1+s/2)} \prod_{\rho} \left( 1 - \frac{s}{\rho} \right) \]

n: integers  
p: primes  
: Riemann zeros

Riemann hypothesis (1859):

the complex zeros of the classical zeta function \( \zeta(s) \) all have real part equal to 1/2

\[ \zeta(s_n) = 0, \ s_n \in C \rightarrow s_n = \frac{1}{2} + iE_n, \ E_n \in \mathbb{R}, \ n \in \mathbb{Z} \]

In fact:
A gas of primes (Julia, Spector, 1990)

Single particle levels

Many particle state of bosons

Total energy

Partition function

\[ Z \text{ diverges at } s=1 \rightarrow \text{Hagedorn transition} \]
The Riemann zeros look like the spectrum of random physical systems

Bohigas, Gianonni (1984)

GUE statistics
Quantum chaos, primes and Riemann zeros

Berry Conjecture (1986):
there exist a classical chaotic Hamiltonian H
Periodic orbits $\rightarrow$ prime numbers $\rightarrow$ periods $= \log p$
Energies $\rightarrow$ Riemann zeros $\rightarrow$ $s = \frac{1}{2} + i \ E$

Proof of the Riemann hypothesis
In previous models the primes are classical objects:

- Energies of Stat Mech (primon gas)
- Periods of orbits (quantum chaos)

Idea: make the primes quantum objects
Quantum Computation and prime numbers
(JIL, GS, 2013)

Classical computer

n bits

\[ x = x_0 2^0 + x_1 2^1 + \ldots x_{n-1} 2^{n-1}, \quad x_i = 0, 1, \quad x = 0, 1, \ldots 2^n - 1 \]

Quantum computer

n qubits

\[ |x\rangle = |x_{n-1}, \ldots, x_0\rangle = |x_{n-1}\rangle \otimes \ldots \otimes |x_0\rangle \]
The Prime State

Primes → State

2 3 5
7 11 ...

is the prime counting function
Quantum Mechanics allows for the superposition of primes implemented as states of a computational basis.

Ex. n=3
Could the Prime state be constructed?

Does it encode properties of prime numbers?

Could it provide the means to explore Arithmetics?

What are its entanglement properties?
Construction of the Prime state (probabilistic)

Efficient construction

PNT
Construction of the Prime state (deterministic)

Grover's search algorithm

Oracle $U_{oracle}|x\rangle = (-1)^{\chi(x)}|x\rangle$

$\chi(x) = 1 (prime), 0 (composite)$

# calls to the oracle
# calls to Grover

Overlap between Grover state and the Prime state

We need to construct an oracle!
Construction of a Quantum Primality oracle

Idea: take a classical primality test and make it quantum-> unitary transformations

Miller-Rabin primality test

- Find \( s \) and \( d \) (odd) such that
- Choose witness \( a \)
- If \( a^d \neq 1 \text{ mod } x \) then \( x \) is composite with certainty
- \( a^{2^r d} \neq -1 \text{ mod } x \) \( 0 \leq r \leq s - 1 \)
- If the test fails, \( x \) may be prime or composite.
- Latter case: \( a \) is a strong liar to \( x \)
- Eliminate strong liars checking less than witnesses
Quantum Counting of Prime numbers

quantum primality oracle + quantum counting algorithm

Brassard, Hoyer, Tapp (1998)

Counts the number of solutions to the oracle
We want to count $M$ solutions out of $N$ possible states.

We know an estimate $\tilde{M}$

$$|\tilde{M} - M| < \frac{2\pi}{c} M^{\frac{1}{2}} + \frac{\pi^2}{c^2}$$

Bounded error in quantum counting

Bounded error in the quantum counting of primes

$$\left| \pi_{QM}(x) - \pi(x) \right| \leq \frac{2\pi}{c} \frac{x^{1/2}}{\log^{1/2} x}$$

We use the PNT
Error of quantum counting < fluctuations under the RH

\[ |\pi_{QM}(x) - \pi(x)| \leq \frac{2\pi}{c} \frac{x^{1/2}}{\log^{1/2} x} \]

Riemann Hypothesis

\[ |Li(x) - \pi(x)| < \frac{1}{8\pi} \sqrt{x \log x} \]

Error of quantum counting < fluctuations under the RH

A quantum computer could falsify the RH, but not prove it !!
Classical versus quantum computation of $\pi(x)$


$$T \sim x^{\frac{1}{2}} \quad S \sim \log x$$

A Quantum Computer could calculate the size of fluctuations more efficiently than a classical computer
Construction of the Twin Prime state

Twin Prime counting function
\[ \pi_2(x) \approx 2 C_2 \frac{x}{(\log x)^2} \]

\[ \Pr(|\text{twin primes}|) = \frac{\pi_2(2^n)}{\pi(2^n)} \approx \frac{2C_2}{n \log 2} \]
Entanglement of a single qubit:

Density matrix qubit $i=1$

Odd primes

$\pi_{4,1} : 5, 13, 17, \ldots \ 4n + 1$

$\pi_{4,3} : 3, 7, 11, \ldots 4n + 3$
Dirichlet theorem:

There infinite number of primes of the form $1 + 4n$ and $3 + 4n$

PNT for arithmetic series

$$\lim_{x \to \infty} \frac{\pi_{4,1}(x)}{Li(x)} = \lim_{x \to \infty} \frac{\pi_{4,3}(x)}{Li(x)} = \frac{1}{\phi(4)} = \frac{1}{2}$$

---

Graph showing the ratio $\pi_{4,1,3}(N)/Li(N)$ with markers indicating $3 \mod 4$ and $1 \mod 4$. The graph suggests a comparison between the two forms of primes with their respective counting functions.
Chebyshev bias:

For low values of $x$ there are more primes $3 \text{ mod } 4$ than $1 \text{ mod } 4$

\[ \Delta(x) = \pi_{4,3}(x) - \pi_{4,1}(x) \]

Chebyshev bias gives the magnetization of qubit $i=1$
Twin primes $(p, p+2)$

Twin primes

$\pi_2^{(1)} : (5, 7), \ldots \ (1 \mod 4, 3 \mod 4)$

$\pi_2^{(3)} : (11, 13), \ldots \ (3 \mod 4, 1 \mod 4)$

Can be measured by off diagonal correlations

$$\langle \sigma_x^{(1)} \rangle = \frac{2\pi_2^{(1)}(2^n)}{\pi(2^n)}, \quad \langle \sigma_x^{(1)} \sigma_x^{(2)} + \sigma_y^{(1)} \sigma_y^{(2)} \rangle = \frac{4\pi_2^{(3)}(2^n)}{\pi(2^n)}$$

Twinship $\rightarrow$ off diagonal entries of density matrix

Sub-series of primes, twin primes, etc. are amenable to measurements
Pairwise correlations between primes  

Counting $p, p+k$ primes $< x$: 

Twin prime constant
If primes were uncorrelated

Prime correlations:

\[ \rho_{n/2} \]

Hardy-Littlewood constant

Toeplitz matrix

GUE statistics of Riemann zeros (Berry, Keating, ..)
Von Neumann entropy of

Volume law scaling
Entanglement spectrum

\[ \rho_{n/2} \sim 1 + \frac{1}{n \log 2} C_{n/2} \quad (n \to \infty) \]

Positive eigenvalues of C matrix
Analytic estimation of entanglement entropy

Renyi entropies can be related to the zeta function

Entanglement properties of the Prime state come from the pairwise Correlations between primes (Hardy-Littlewood conjecture)
Scaling of entanglement entropy

Random states

Prime state

Area law in d-dimensions

Critical scaling in d=1 at quantum phase transitions

Finitely correlated states away from criticality
Conclusions

- The Prime state provides a link between Number Theory and Quantum Mechanics

- Quantum Computers could be used as Quantum Simulators of Arithmetics

- Arithmetic properties could be measured more efficiently than with classical algorithms, e.g. to falsify the Riemann hypothesis

- Entanglement in the Prime state captures fundamental properties as pair correlations between the primes

- Possible connections with Random Matrix Theory, Quantum Chaos and the Riemann zeros
Thank you