Quantum Computation of Prime Number Functions

Germán Sierra
In collaboration with José Ignacio Latorre and Alex Monras
IFT-UAM-CSIC and UB, Singapore

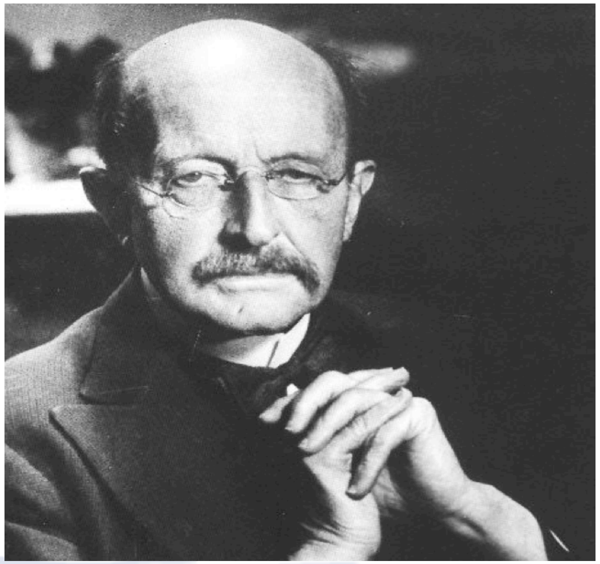
Joint workshop:
Quantum Physics: from fundamental questions to applications
22-24 May 2013, Barcelona, Spain

CLASSICAL PHYSICS

MATHEMATICS

$\mathbb{R}$

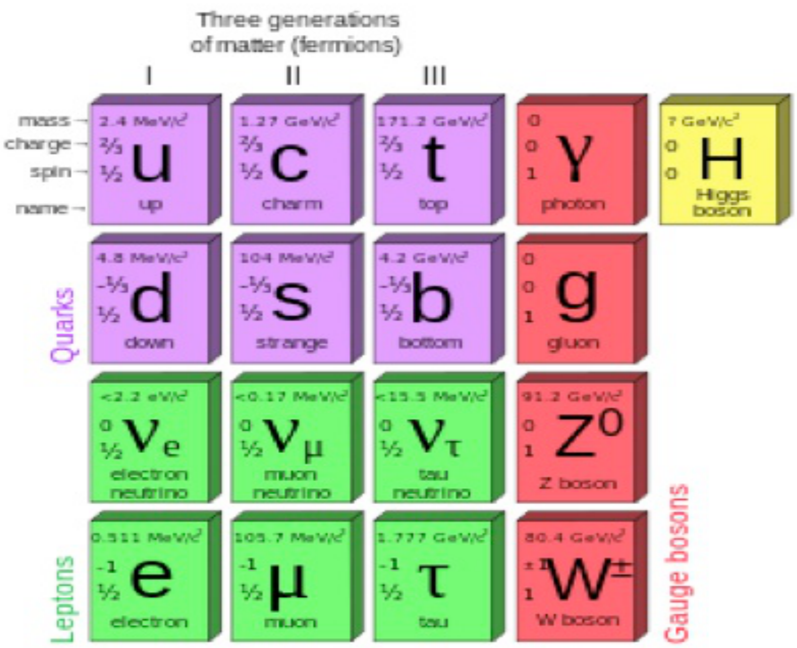
QUANTUM PHYSICS



N

Fundamental building blocks

NATURE



NUMBERS

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

In some sense quantum theory is a bending of physics towards number theory. However, deep facts of number theory play no role in questions of quantum mechanics....

In particular we do not know of any fundamental physical theories that are based on deep facts in number theory.

I would think that quantum mechanics will be completely reformulated and that number theory will play a key role in this formulation.

C. Vafa (2000)

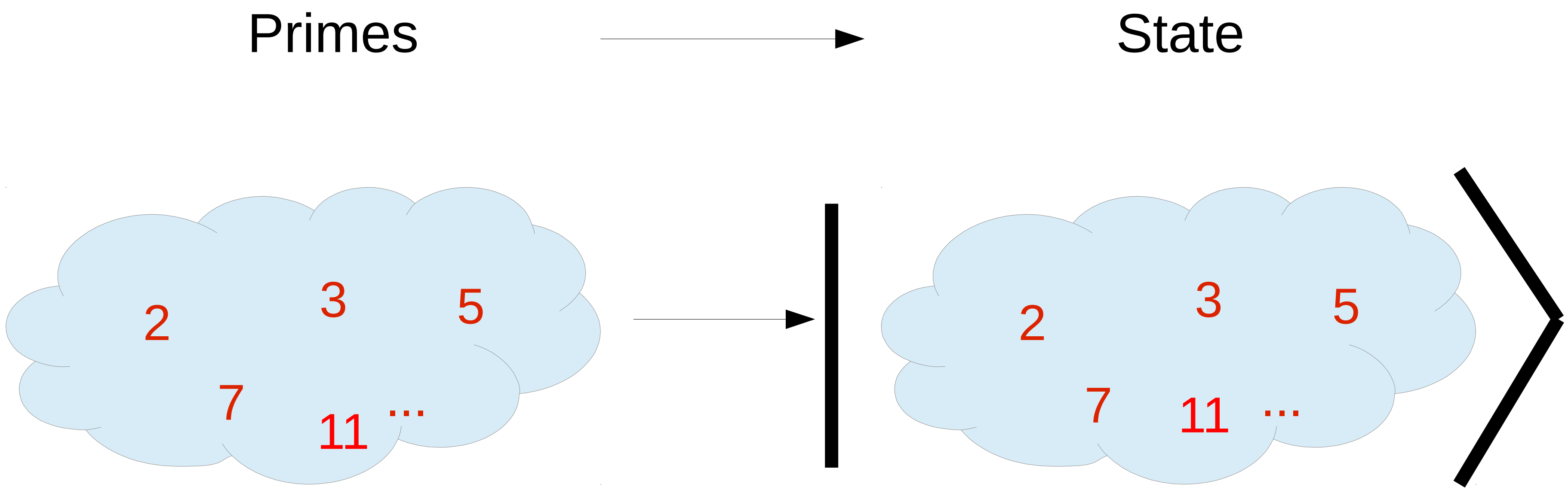
While we wait for this reformulation
let us see if Quantum Mechanics
can do something for Number Theory

Classical computer

n bits $x = x_0 2^0 + x_1 2^1 + \dots x_{n-1} 2^{n-1}, \quad x_i = 0,1, \quad x = 0,1,\dots 2^n - 1$

Quantum computer

n qubits $|x\rangle = |x_{n-1},\dots,x_0\rangle = |x_{n-1}\rangle \otimes \dots \otimes |x_0\rangle$


Primes
State
2
3
5
7
11 ...
2
3
5
7
11 ...

The Prime State

$$|P(n)\rangle = \frac{1}{\sqrt{\pi(2^n)}} \sum_{p<2^n \in Primes} |p\rangle$$

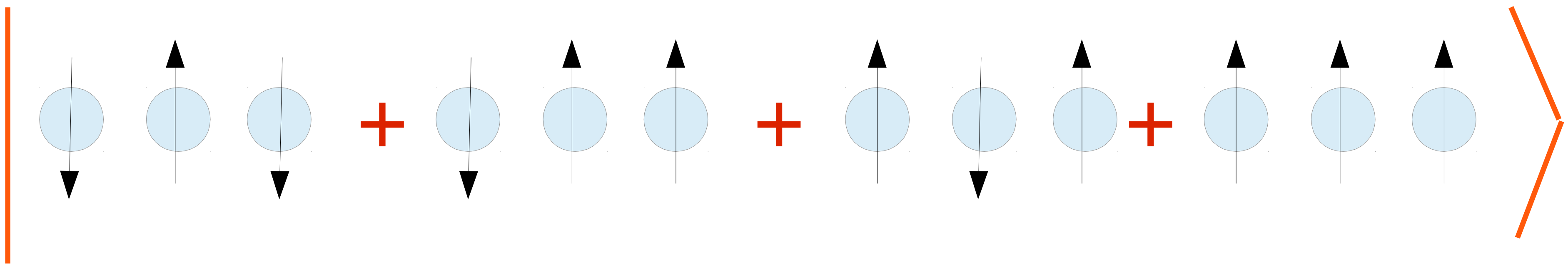
$\pi(2^n)$ is the prime counting function

Quantum Mechanics allows for the superposition of primes implemented as states of a computational basis

$$|P(n)\rangle = \frac{1}{\sqrt{\pi(2^n)}} \sum_{p<2^n \in Primes} |p\rangle$$

Ex. n=3

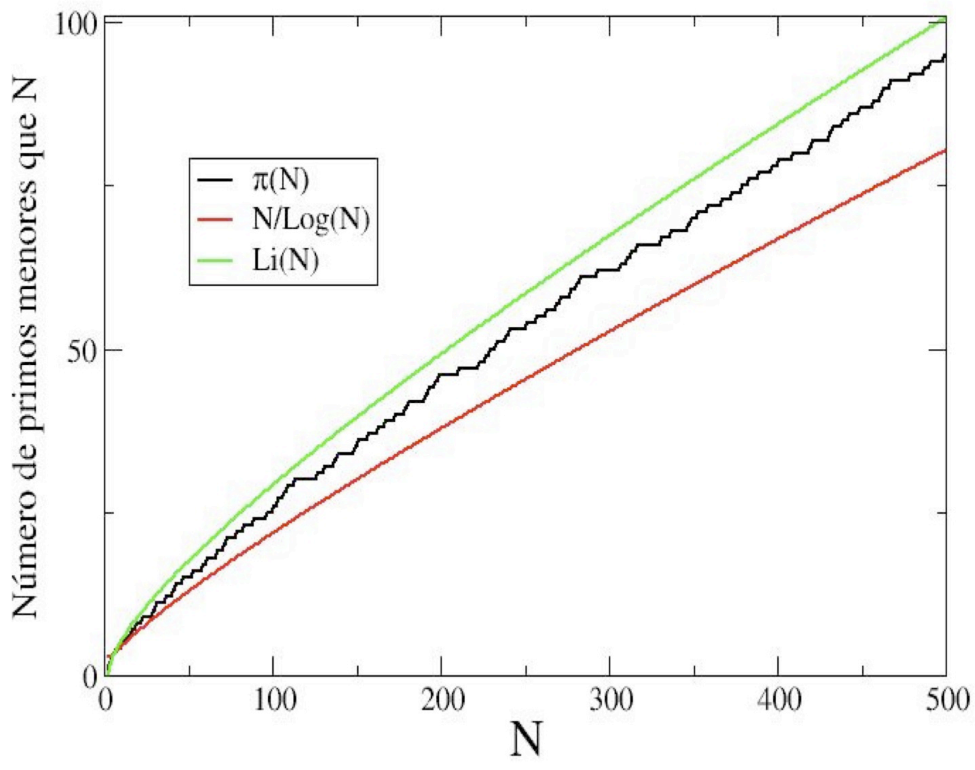
$$|P(3)\rangle = \frac{1}{\sqrt{4}} \left(|2\rangle + |3\rangle + |5\rangle + |7\rangle \right)$$



Prime counting function

$\pi(x)$ Number of primes p less than or equal to x e.g. $\pi(100) = 25$

Gauss – Legendre law



$$\pi(x) \approx Li(x) \approx \frac{x}{\ln x}$$

$$x \to \infty$$

Prime number theorem

- Hadamard (1896)
- de la Vallee-Poussin

Prime Number Theorem (PNT)

$$\pi(x) \approx Li(x) \qquad Li(x) = \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x} + \frac{x}{\log^2 x} + \dots$$

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

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

Platt (2012)

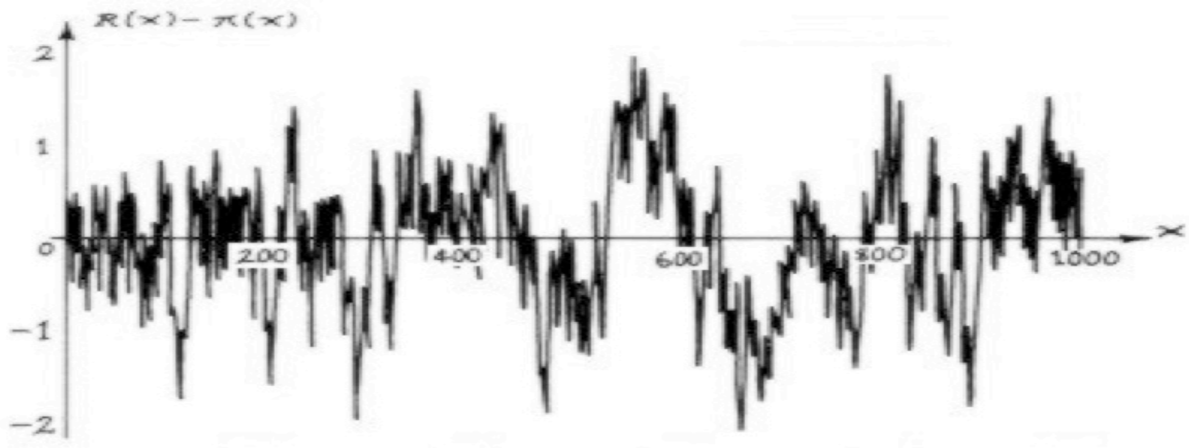
$$Li(10^{24}) - \pi(10^{24}) \approx 1.7\ 10^{10}$$

The prime number function will oscillate around the Log Integral infinitely many times
Littlewood, Skewes

A first change of sign is expected for some $x < e^{727.9513468} \dots$

If the Riemann hypothesis (RH) is correct, fluctuations are bounded

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



$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ If $\zeta(s)=0$ with $0 \leq Real(s) \leq 1$ then $Real(s) = \frac{1}{2}$

Could the Prime state be constructed?

Does it encode properties of prime numbers?

What are its entanglement properties?

Could it provide the means to explore Arithmetics?

Entanglement: single qubit reduced density matrices

$$|P(n)\rangle = \frac{1}{\sqrt{\pi(2^n)}} \sum_{i_{n-1},\dots,i_1,i_0=0,1} p_{i_{n-1}\dots i_1 i_0} |i_{n-1},\dots,i_1,i_0\rangle$$

$$p_{i_{n-1}\dots i_1 i_0} = \begin{cases} 1 & p = i_{n-1}2^{n-1} + \dots + i_0 = prime \\ 0 & otherwise \end{cases}$$

Density matrix qubit i=1

$$\rho_{ab}^{(1)} = \frac{1}{\pi(2^n)} \sum_{i_{n-1},\dots,i_2,i_0=0,1} p_{i_{n-1},\dots,i_2,a,i_0}\, p_{i_{n-1},\dots,i_2,b,i_0}$$

$$\rho_{00}^{(1)} = \frac{\pi_{4,1}(2^n)}{\pi(2^n)} \qquad \rho_{11}^{(1)} = \frac{1+\pi_{4,3}(2^n)}{\pi(2^n)} \qquad \rho_{01}^{(1)} = \frac{\pi_2^{(1)}(2^n)}{\pi(2^n)}$$

Odd primes

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

$$\pi_{4,3} : 3, 7, 11, \dots \; 4n+3$$

Dirichlet theorem:

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

PNT for arithmetic series

$$\lim_{x\to\infty}\frac{\pi_{4,1}(x)}{Li(x)} = \lim_{x\to\infty}\frac{\pi_{4,3}(x)}{Li(x)} = \frac{1}{\phi(4)} = \frac{1}{2} \longrightarrow S\left(\rho^{(i)}\right)\sim\log 2$$

Chebyshev bias:

For low values of x there exist more primes 1 mod 4 than 3 mod 4

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

Related to magnetization of qubit i=1 $\quad \langle \sigma_z^{(1)} \rangle = \dfrac{-\Delta(2^n)-1}{\pi(2^n)}$

Twin primes : p, p+2

Counting function $\pi_2(x) \approx 2C_2 \dfrac{x}{(\log x)^2}$ (Hardy-Littlewood conjecture)

Twin primes

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

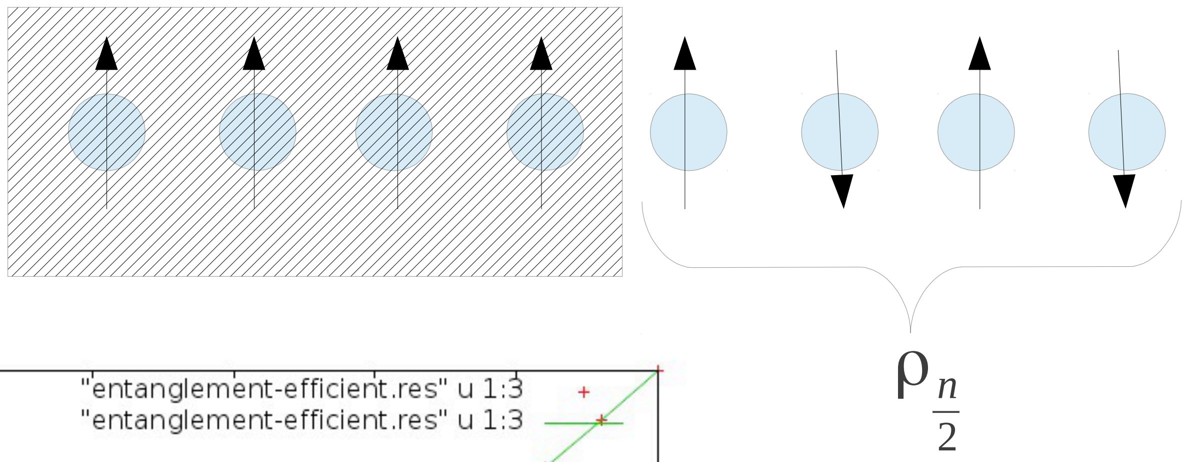
$$\pi_2^{(3)} : (11,13),\ldots \quad (3 \bmod 4,\ 1 \bmod 4)$$

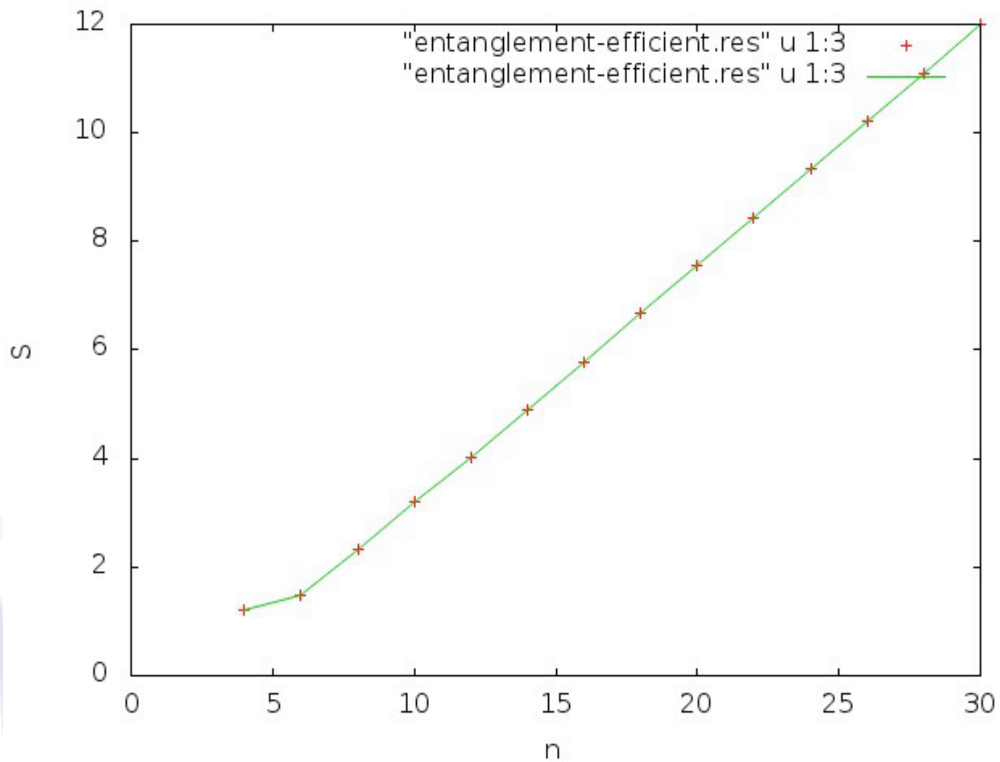
$$\left\langle \sigma_x^{(1)} \right\rangle = \frac{2\pi_2^{(1)}(2^n)}{\pi(2^n)}, \qquad \left\langle \sigma_x^{(1)}\sigma_x^{(2)} + \sigma_y^{(1)}\sigma_y^{(2)} \right\rangle = \frac{4\pi_2^{(3)}(2^n)}{\pi(2^n)}$$

Twinship → off diagonal entries of density matrix

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

Entanglement entropy of the Prime state





“There is entanglement in the Primes”

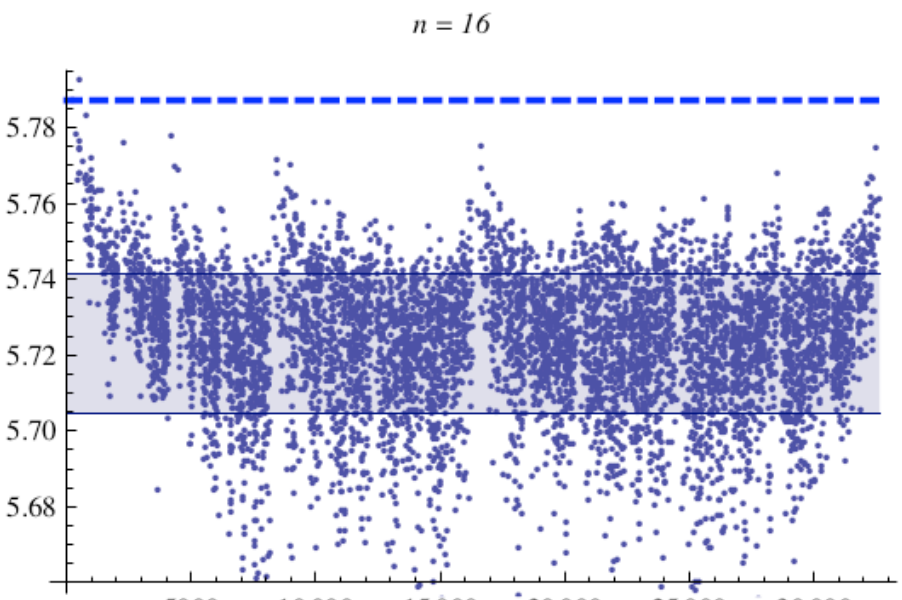
Volume law scaling

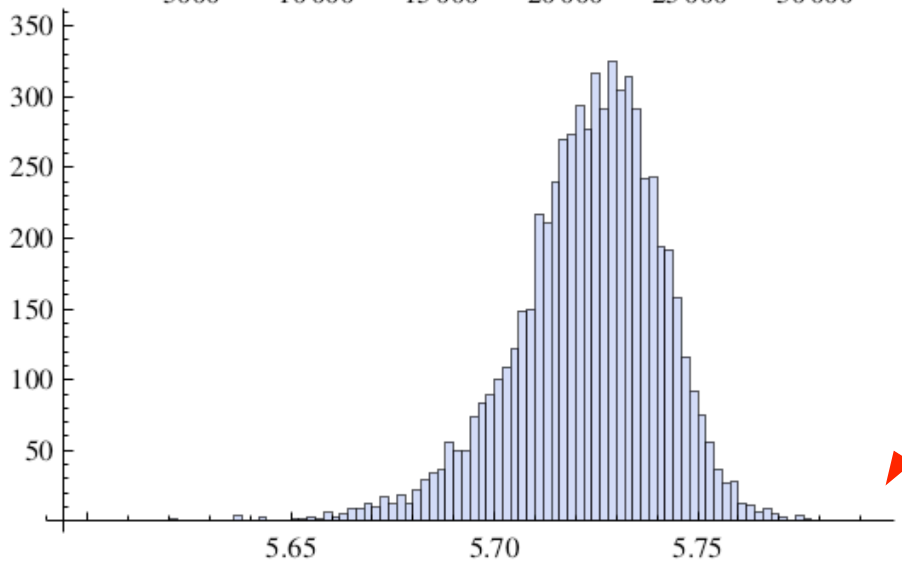
$$S \sim .8858\, n + const$$

A. Monras, G. Sierra, JIL

Scaling of entanglement entropy

$S \sim n - const$	Random states
$S \sim .8858\, n + const$	Prime state
$S \sim n^{\frac{d-1}{d}} + const$	Area law in d-dimensions
$S \sim \frac{c}{3} \log n + const$	Critical scaling in d=1 at quantum phase transitions
$S \sim \log(\xi) = const$	Finitely correlated states away from criticality



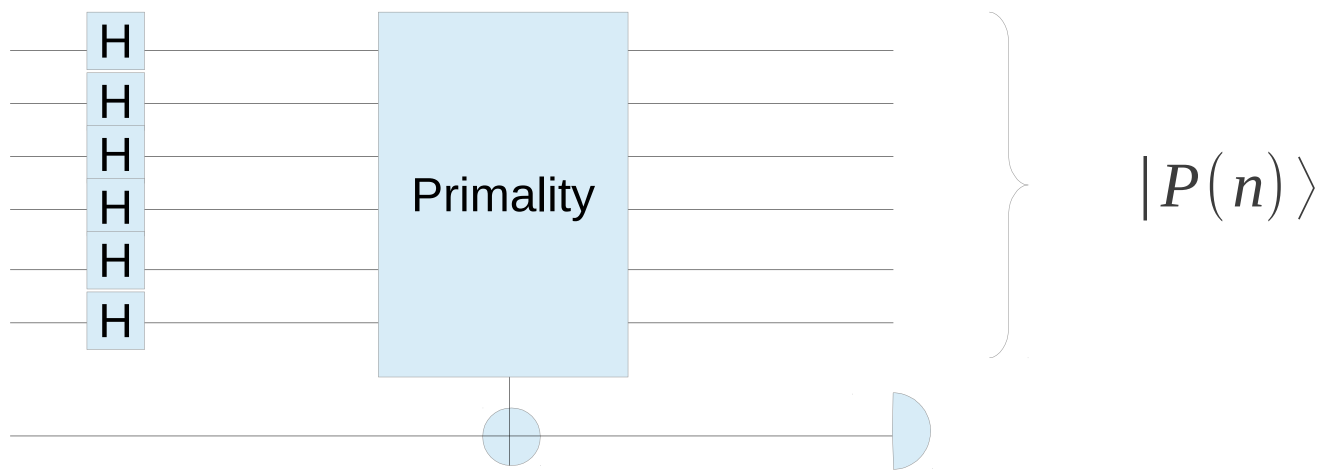


$$\mu = 5.72307; \quad \sigma = 0.0184293; \quad \frac{S_{\max} - \mu}{\sigma} = 3.47743$$

Entanglement entropy
for different partitions

Original partition carries
more entanglement (!!?)

Construction of the Prime state



$$U_{primality} \sum_x |x\rangle|0\rangle = |P(n)\rangle|0\rangle + \sum_{c \in composite} |c\rangle|1\rangle$$

$$Prob(|P(n)\rangle) = \frac{\pi(2^n)}{2^n} \approx \frac{1}{n \log 2}$$

Efficient construction

Construction of twin primes

$$U_{+2}|P(n)\rangle|0\rangle = \sum_{p \in primes} |p+2\rangle|0\rangle$$

$$U_{primality} U_{+2}|P(n)\rangle|0\rangle = \sum_{p,\, p+2 \in primes} |p+2\rangle|0\rangle + \sum_{p+2 \notin primes} |p+2\rangle|1\rangle$$

$$\Pr(|twin\ primes\rangle) = \frac{\pi_2(2^n)}{\pi(2^n)} \approx \frac{2C_2}{n\log 2}$$

Grover construction of the Prime state

$$|\psi_0\rangle = \sum_{x<2^n} |x\rangle = \frac{1}{\pi(2^n)} \Big(\overbrace{\sum_{p\in primes} |p\rangle}^{M} + \sum_{c\in composites} |c\rangle \Big)$$

$$\underbrace{\hphantom{\sum_{p\in primes} |p\rangle + \sum_{c\in composites} |c\rangle}}_{N}$$

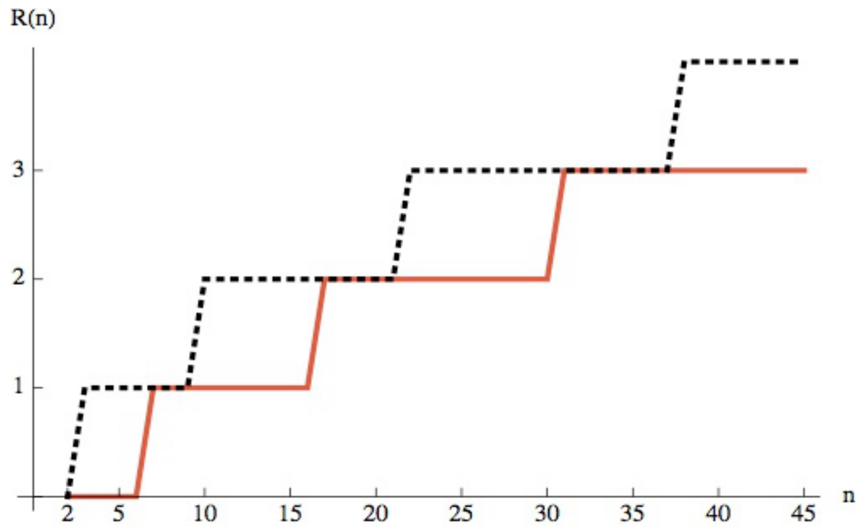
$$\Big\downarrow$$

calls to Grover

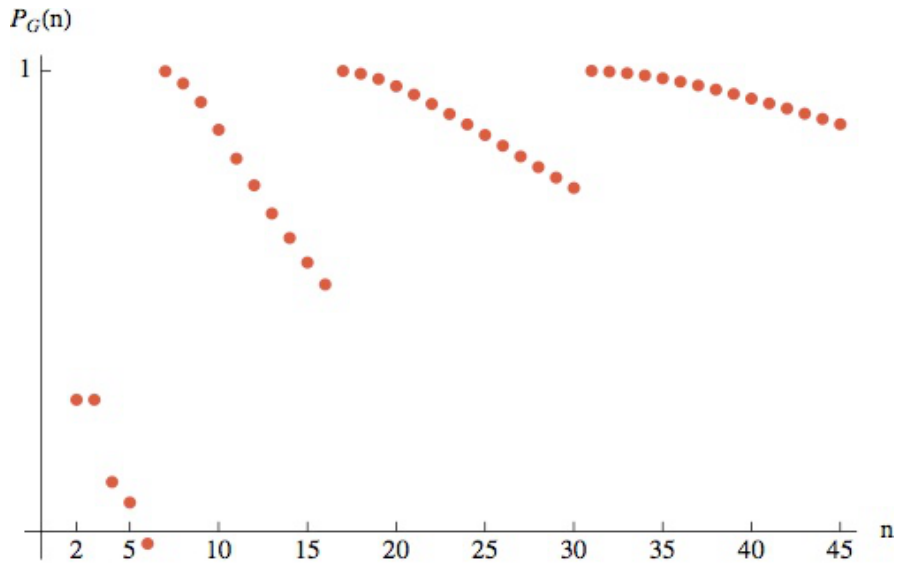
$$R(n) \le \frac{\pi}{4}\sqrt{\frac{N}{M}} \le \frac{\pi}{4}\sqrt{n\log 2}$$

$$|\psi_f\rangle = |P(n)\rangle$$

calls to Grover



Overlap between
Grover state and the Prime state



We need to construct an oracle!

Construction of a Quantum Primality oracle

An efficient Quantum Oracle can be constructed using classical primality tests

Miller-Rabin primality test

- Find s and d (odd) such that

$$x \rightarrow x-1=2^s d$$

- Choose witness a

$$1 \leq a \leq x$$

- If $a^d \neq 1 \bmod x$ then x is composite with certainty

$$a^{2^r d} \neq -1 \bmod x \qquad 0 \leq r \leq s-1$$

- 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 $\log^2 x$ witnesses

Construction of a Quantum Primality oracle

An efficient Quantum Oracle can be constructed using classical primality tests

Miller-Rabin primality test

- Find s and d (odd) such that

$$x \rightarrow x-1=2^s d$$

- Choose witness a

$$1 \leq a \leq x$$

- If $a^d \neq 1 \, mod \, x$ then x is composite with certainty

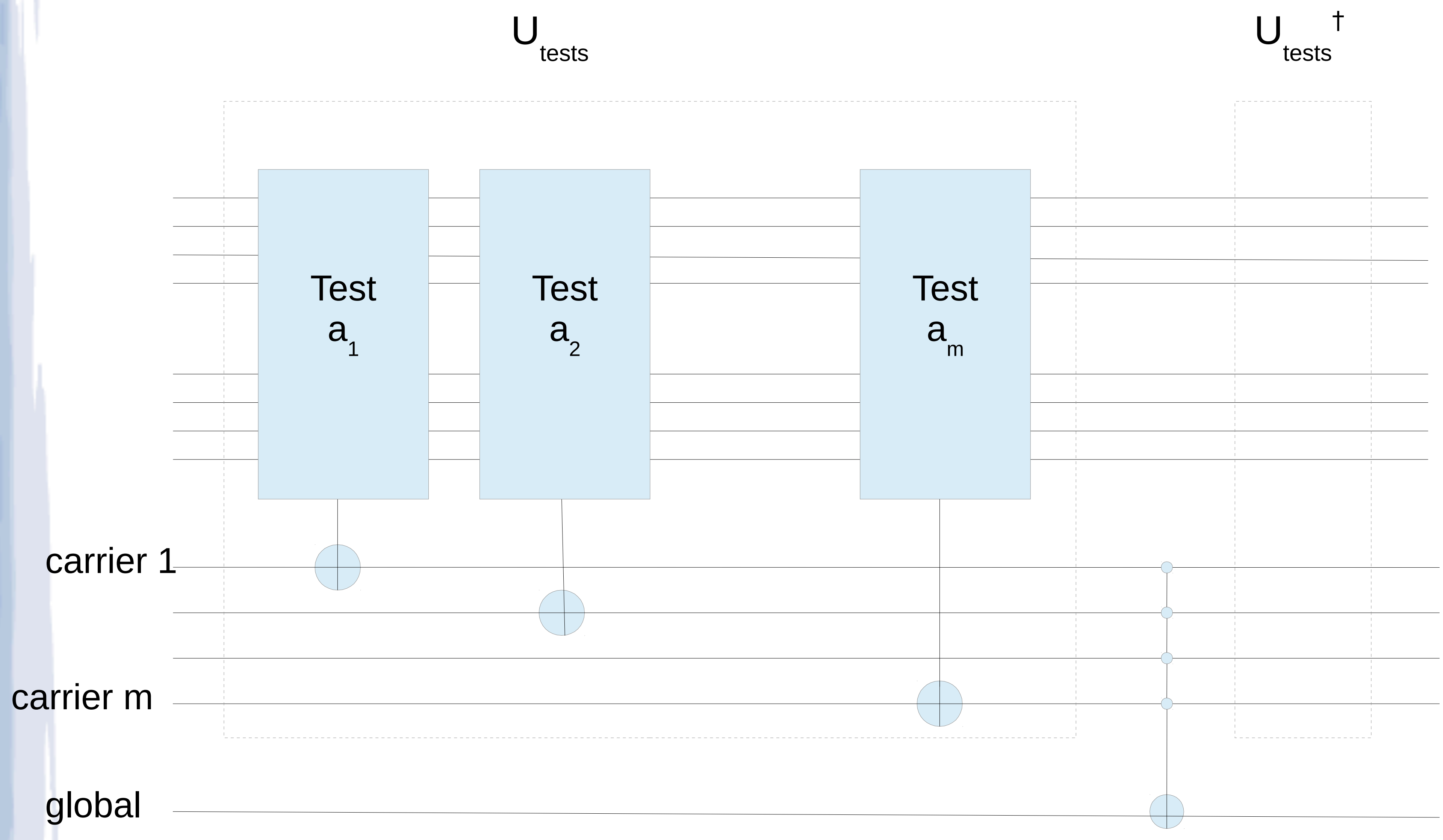
$$a^{2^r d} \neq -1 \, mod \, x \qquad 0 \leq r \leq s-1$$

- 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 $\log^2 x$ witnesses

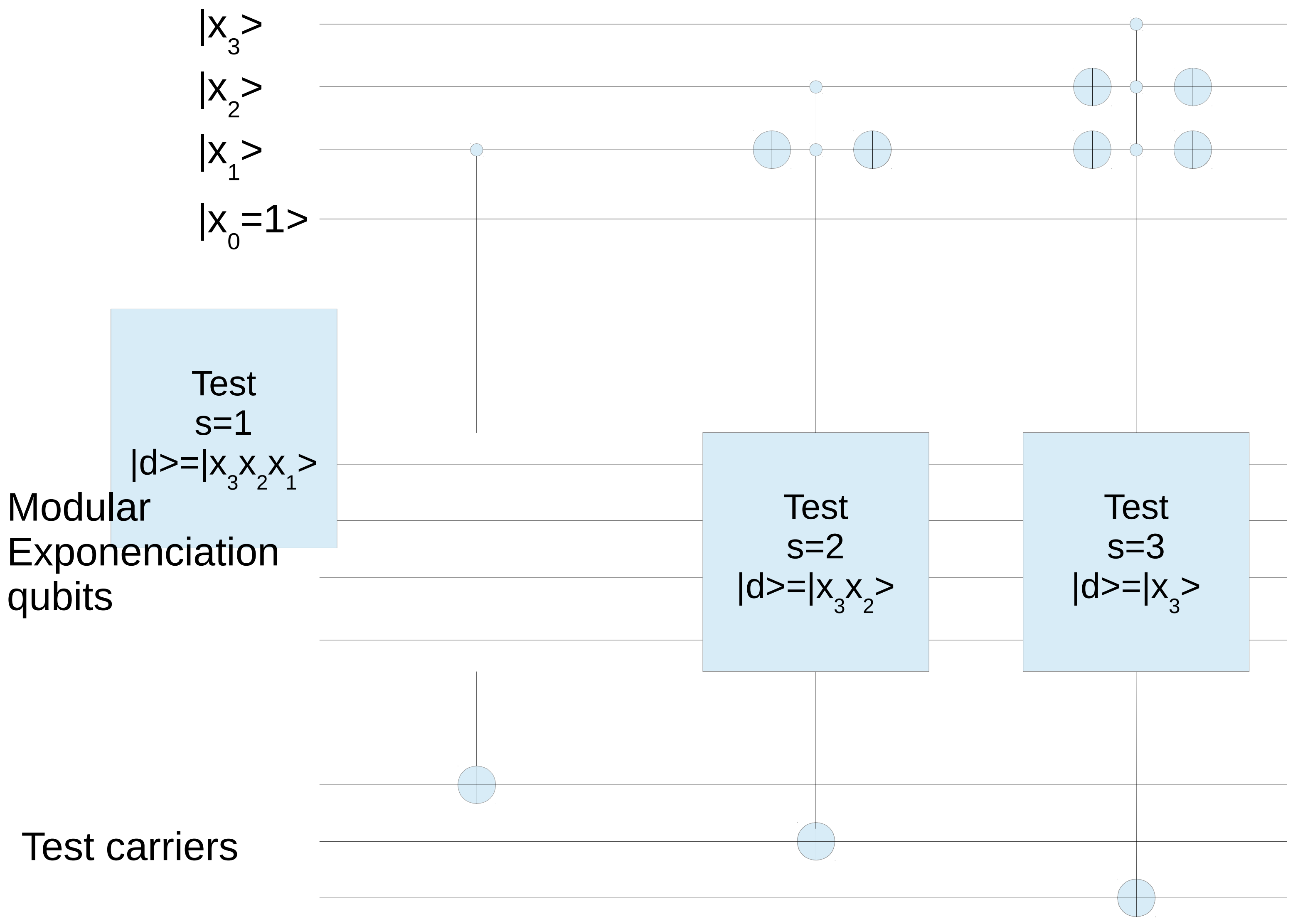
Finding d and s

$$x = 49 \rightarrow x - 1 = 48 = 2^4 \times 3 \rightarrow s = 4, d = 3$$

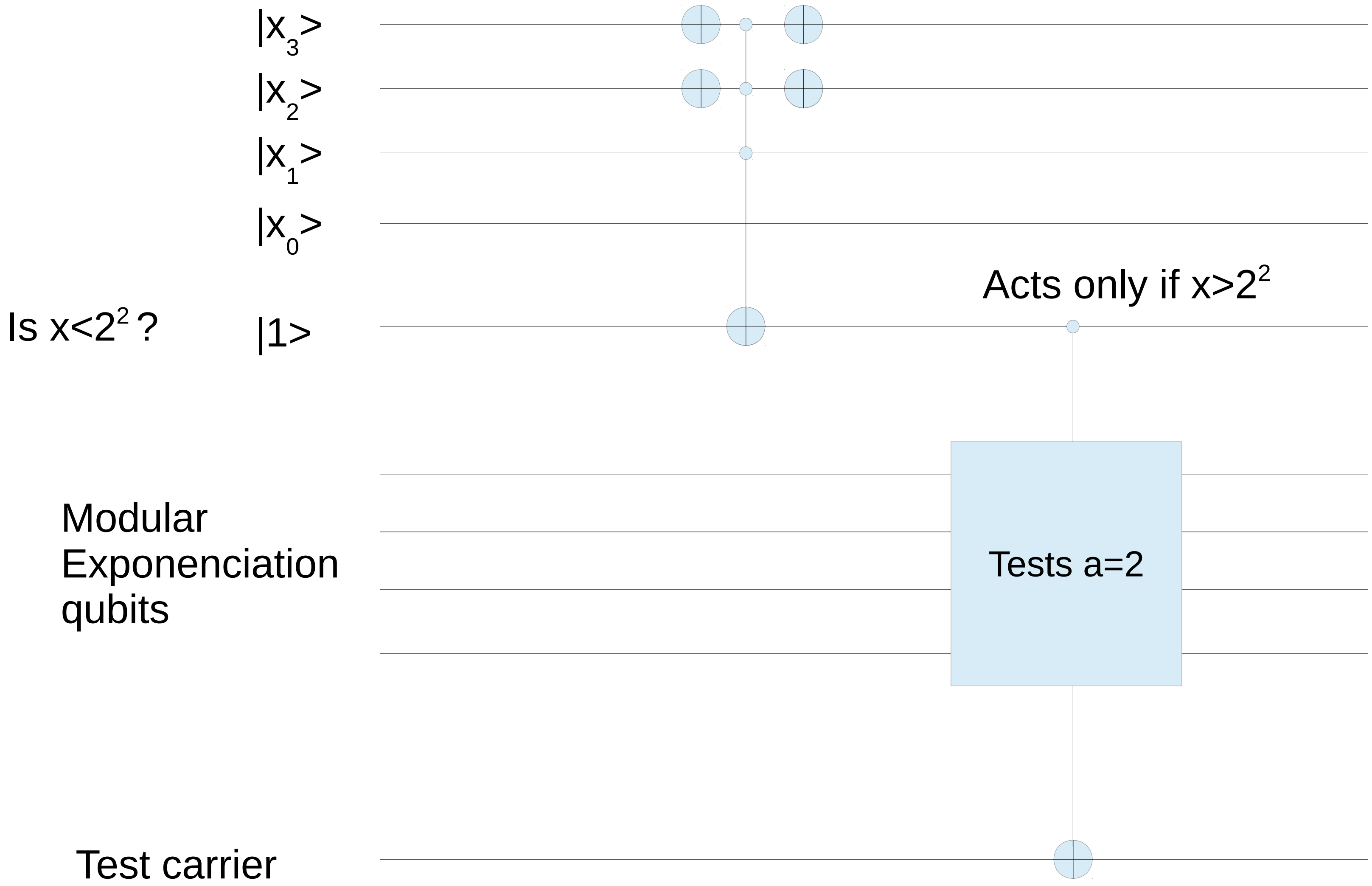
$$|49\rangle = |1,1,0,0,0,1\rangle \rightarrow |\underbrace{1,1}_{d},\underbrace{0,0,0,0}_{s}\rangle$$



Structure of the quantum primality oracle



Tests are condition to the actual value of *x*

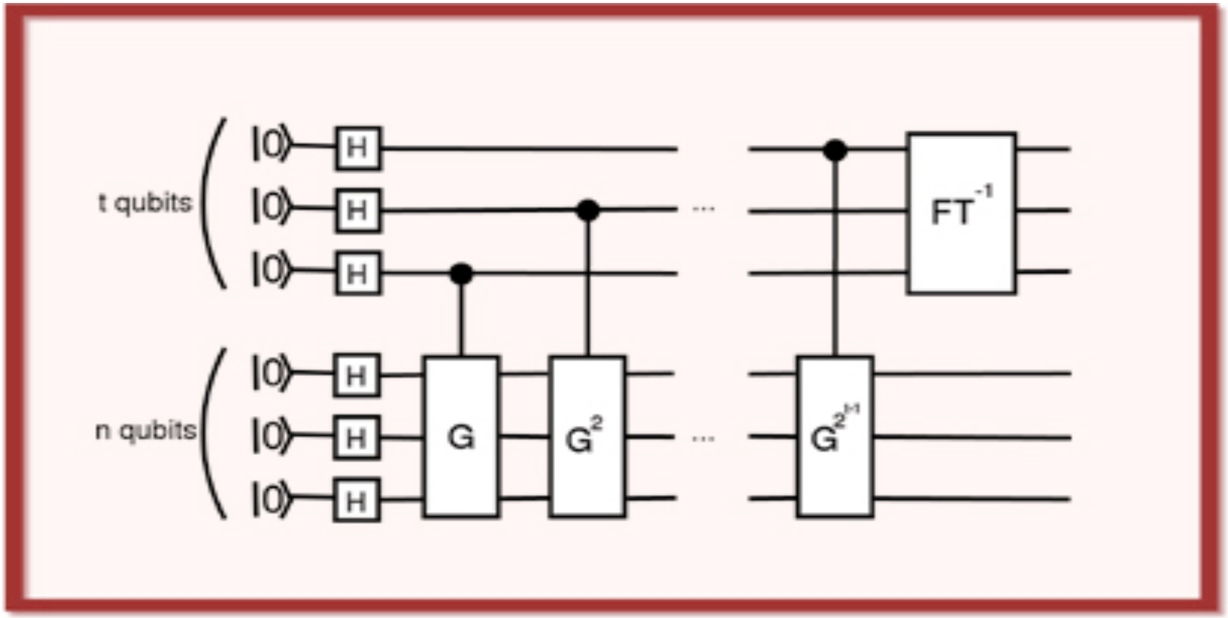


Tests are only run when witness is smaller than x

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

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

We use the PNT

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

Error of counting is smaller than the bound
for the fluctuations if Riemann hypothesis is correct

$$\frac{2\pi}{c} \frac{x^{\frac{1}{2}}}{\log^{\frac{1}{2}} x} < x^{\frac{1}{2}} \log x$$

Best classical algorithm by Lagarias-Miller-Odlyzko (1987)
implemented by Platt (2012)

$$T \sim x^{\frac{1}{2}} \qquad S \sim x^{\frac{1}{4}}$$

A Quantum Computer could calculate the size of fluctuations more efficiently than a classical computer

$$T \propto x^{\frac{1}{2}} \qquad S \propto \log x$$

Beyond Prime numbers: the **q-functor**

$$S \subseteq X \to |S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in S} |x\rangle$$

$$|S\rangle = \frac{1}{\sqrt{|S|}} \sum_{x \in X} \chi_S(x) |x\rangle \qquad \chi_S(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$$

Primes
Average (Cramér) primes
Dirichlet characters
...

Only needs the construction of a quantum oracle for **χ_S(x)**

Conclusion

Quantum Simulation of Arithmetics

- Superposition of series of numbers using appropriate q-oracles
- Measurements of arithmetic functions
- More efficient approaches are likely

Thank you

Gracies

What is this?

Gaudi Magic Square
in Sagrada Familia
Barcelona