Quantum Computing at CERN

INFN and the future of Scientific Computing

Federico Carminati

May 4th, 2018

Outline

What is Quantum Computing (in a nutshell)?

Where are we now?

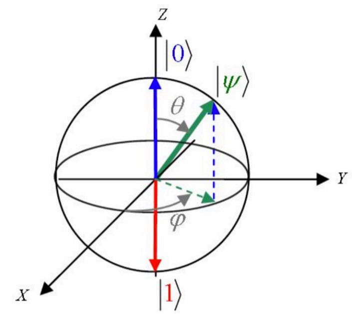
What could be in for HEP?

What are we doing about it?

Quantum Computing?

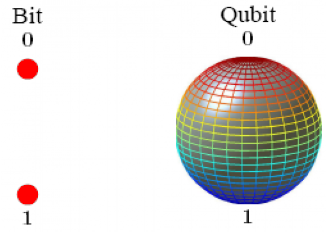
"Nature is quantum, goddamn it! So if we want to simulate it, we need a quantum computer."
R.Feynman, 1981, Endicott House, MIT

Use qubits instead of bits… e.g. bits that exhibit quantum behavior



`Bloch's sphere

Qubits are great!

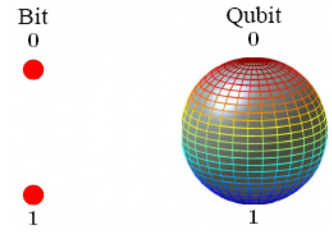


n normal bits can be in one of 2^n states at a time

n qbits can be in 2^n states at the same time: any quantum operation is in fact 2^n operations **in parallel**

…and the icing on the cake is *entanglement* of the qubits: any operation on one part of the set has implications on the other

But qubits are also nasty…



Extremely difficult to realize in practice

You can only retrieve one quantum state at a time

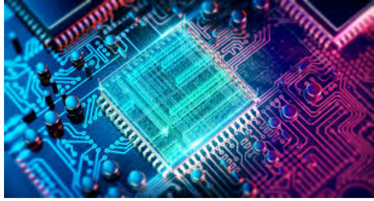
States cannot be copied exactly

You can only use reversible (Unitary) logic gates, limiting the algorithms you can apply

Quantum decoherence is always present

Errors are more difficult to correct (you have to correct the phase too)

Quantum Computing in perspective



The three frontiers

- Short distance -> High Energy Physics
- Long distance -> Cosmology
- Entanglement (i.e. complexity) -> Quantum Information Technology

Since Turing it was believed that the “hardness” of a problem (whether it could be solved in polynomial or greater time), was independent of the physi-cal apparatus

This basic concept of Computer Science is now challenged by quantum computers

Quantum supremacy (or is the gain worth the pain?)

Can we control complex quantum systems and if we can, so what?
(J.Preskill, 2012)

Can quantum computers outperform classical computers on all algorithms?

Can quantum computers do things that cannot be done by classical computers (quantum supremacy)?

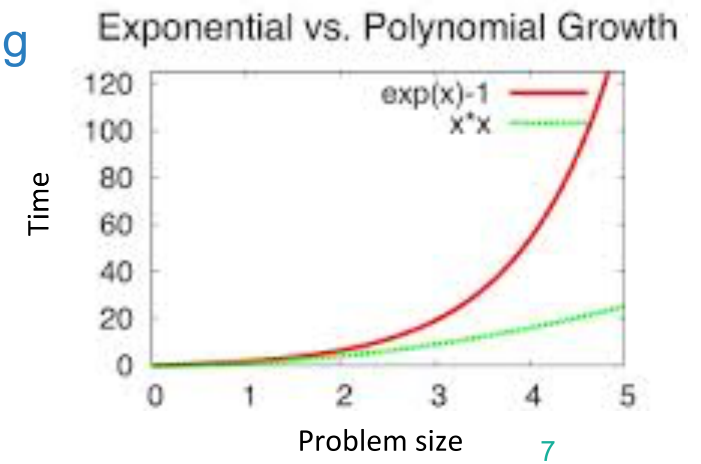
The golden apple is "superpolynomial speedup"

- Reducing to polynomial time what in classic computing is exponential or more
- Theoretically achieved with some algorithms

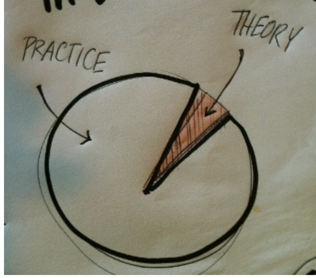
But also polynomial speedup can be very appealing

- Particularly for large problems

For the moment it is debatable whether Quantum Supremacy has been demonstrated or not



Early quantum algorithms



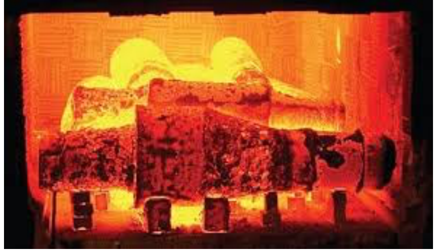
Integer factorization (Shor's algorithm): $\sim \exp(O(\log N)) \Rightarrow O((\log N)^3)$

- Special case of Hidden Subset Pproblem
- Beware cryptography algorithms (blockchain, RSA, Diffie-Hellman, DSA, ECDH, ECDSA, Buchmann-Williams NTRU, Ajtai-Dwork)

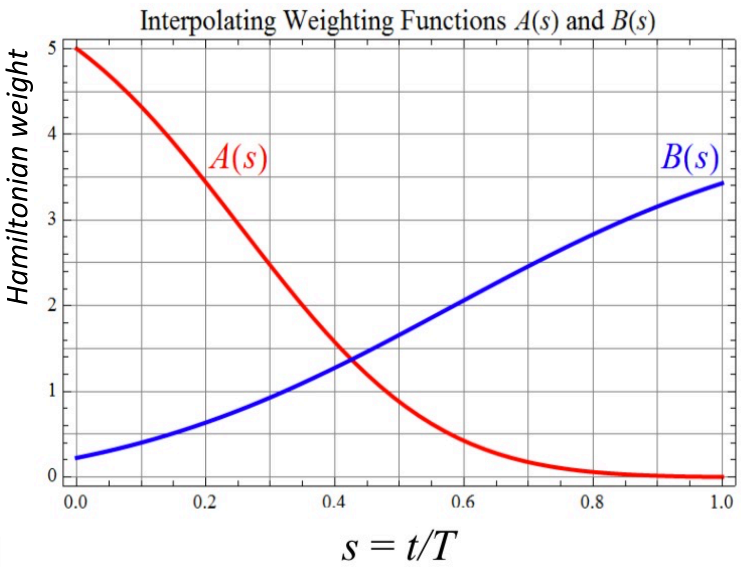
Unstructured search problem (Grover's algorithm): $\sim O(N) \Rightarrow O(\sqrt{N})$

- Can solve all NP problems, e.g. many important problems involving optimization and constraint satisfaction
- Minimum of unsorted integer list, graph connectivity and pattern matching

Adiabatic optimization



D-Wave
The Quantum Computing Company™



Can be applied to any constraint satisfaction problem (CSP), based on a correspondence between CSPs and physical systems

Start with a uniform superposition over all possible solutions to the CSP and adiabatically evolve it to a state encoding the solution, always in ground state

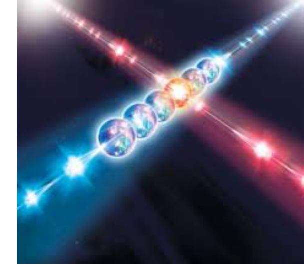
$$\mathcal{H}(s) = A(s)\sum_i \sigma_i^x + B(s)\left[\sum_i a_i\,\sigma_i^z + \sum_{i<j} b_{ij}\,\sigma_i^z\sigma_j^z\right]$$

No need of quantum gates… however no theoretical upper bound

In reality the Hamiltonian does not remain in its ground state, so the system is rather performing a "quantum annealing"

The D-Wave system has now 2000 (non quantum gated!) bits

Quantum Simulation



The first application imagined for Quantum Computers (Feynman 1981)

Given a Hamiltonian H describing a physical system, and a description of an initial state |ψ⟩ of that system, output some property of the state $|\psi(t)\rangle = e^{-iHt}|\psi\rangle$

The exponential complexity of a general quantum states makes this problem impossible to be solved classically

Digital Quantum Simulation:

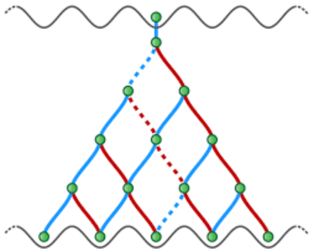
- In a General Purpose quantum computer, given a description of a quantum state |ψ⟩, a description of H, and a time t, the quantum simulation algorithm produces an approximation to the state |ψ(t)⟩ where measurements can be performed
- Speedup is superpolynomial
- Very active field of research… no actual realization yet

Precise molecular design can be a game changer here!

Analog Quantum Simulation:

- Mimic one physical system directly using an approximating one, easier to build and measure.

Quantum Walks



Simulated coherent quantum evolution of a particle moving on a graph

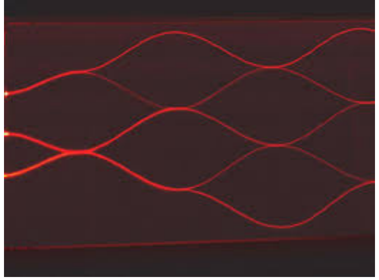
Square or even logarithmic speedup

All algorithms based on Markov chains

- In particular Markov chain based search algorithms

Fast evaluation of Boolean expression trees

Quantum Sampling



We can obtain very fast quantum sampling of a state vector x in the following way

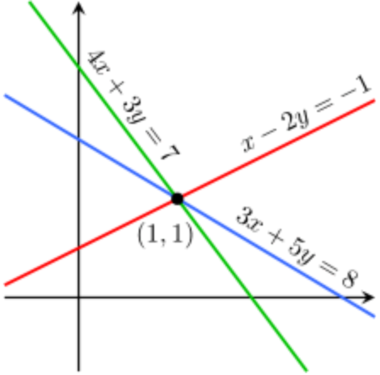
- Prepare a state $|0\rangle$
- Subject this to a unary evolution via a quantum circuit C
- Measure the system in the computational basis

The computation outputs a length n bitstring $x \in \{0, 1\}^n$ with probability

$$p_x = |\langle x|C|0\rangle|^2$$

So we have produced a probabilistic sample from a distribution determined by the circuit C

Linear systems



Ax=b can be solved classically in polynomial time

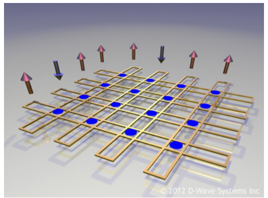
Harrow, Hassidim and Lloyd have shown that they can produce an approximate $|x\rangle = \sum_{i=1}^{N} x_i |i\rangle$ in $O(\log N)$

However measuring each x_i will still be linear in N (at least)

But we might not need each x_i, but some global property

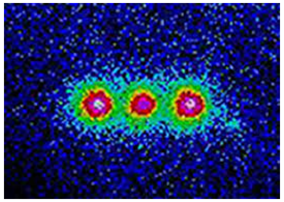
Current hardware options

Wire loops and Josephson's junctions (D-Wave)



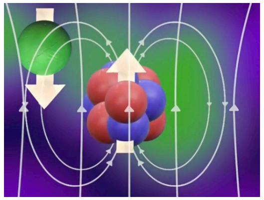
- Flow of current UP and DOWN
- Junction used to set and read the qubit

Ion Traps



- An atom is (laser) cooled down and used as a qubit
- The status is set and read via a laser

Single atom impurities (Phosphorus) in a silicon matrix



- Atom is used as a qubit
- A mag field is used to set and read the qubit

Intrinsic limit?

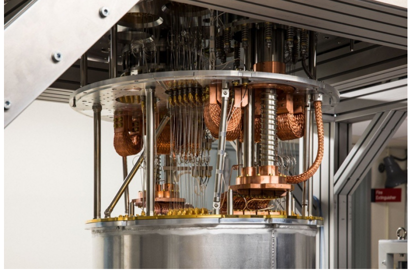
’t Hooft (1993) and Susskind (1995) have proposed the *holographic principle:* the information content of the entire universe is captured by an enveloping surface that surrounds it

A *simple* calculation of the size of our universe’s event horizon today based on the measured value of dark energy gives an information bound of 10^{122} bits

A quantum computer with 400 qbits will require more bits of information to define it than can be accommodated in the entire observable universe!

What will happen if…

Current hardware status



D-Wave system has one 2000 qubit Quantum Annealing computer running at a customer site
https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order

Price tag 15M$

IBM has a announced a 50 qubits computer February 2018
https://www.technologyreview.com/s/610250/hello-quantum-world/

Google has announced a 72 qubits computer March 2018
https://www.technologyreview.com/s/610274/google-thinks-its-close-to-quantum-supremacy-heres-what-that-really-means/

What's in for us

Most of the work we do is based on optimisation / fitting / minimisation which features superpolynomial speedup

Training of Deep Learning is more and more revealing to be a bottleneck, quantum computing can substantially speed it up https://www.datasciencecentral.com/profiles/blogs/quantum-computing-deep-learning-and-artificial-intelligence

Combinatorial searches can be speeded up (track reconstruction)

We can simulate basic interactions with QC, see https://www.nature.com/news/quantum-computer-makes-first-high-energy-physics-simulation-1.20136

Lattice QCD calculations https://mappingignorance.org/2017/01/27/simulating-particle-physics-quantum-computer/

Very fast random number generators can be built

How do we go about it?

Contact various vendors interested to work with us in the context of CERN openlab

Collect use-cases from interested users

Establish pilot projects with vendors

We will have a kickstart brainstorming on November 5-6
https://indico.cern.ch/event/719844/

Conclusions

Quantum computing seems to be behind the curve

Potentially it could provide substantial benefits to our field

It is the right time for HEP to get involved

CERN openlab has a long and successful experience of engaging with industry to bring new technologies to HEP

See you in November!

Benchmarking

- Only few papers published on D-Wave systems discuss performance
  - Previous- generation processors too small and when problems are small, classical and quantum solvers are uniformly fast
- Two recent papers
  - Trummer and Koch, working on DataBases searches report that the best of five classical solvers can be up to 1000 times slower than a D-Wave 2X system.
  - Ushijima-Mwesigwa et al. report that quantum and hybrid classical quantum matrix decomposition implemented on current systems can equal or outperform state of the art classical methods