DA VINCI DIALOGUES SÉMINAIRE DEEP TECH

9-10 AVRIL 2024

S

CHÂTEAU LOUISE DE LA VALLIÈRE REUGNY, INDRE-ET-LOIRE

À LA DÉCOUVERTE DES TECHNOLOGIES QUANTIQUES

Olivier Ezratty



à la découverte des technologies quantiques

olivier ezratty

{ auteur | ... }
Tours, 10 avril 2024
olivier@oezratty.net www.oezratty.net @olivez

14 May 2018

Alain Aspect

Fanny Bouton at OVHcloud since June 2020

sciences used with quantum technologies



physics

electromagnetism quantum physics quantum matter thermodynamics fluids mechanics photonics



engineering

materials design

electronics engineering cryogenics mathematics linear algebra groups theory analysis complexity theories



π

computer science

information theory algorithms design programming classical computing telecommunications machine learning

human sciences philosophy epistemology sociology technology ethics economics of innovation R&D policy making geopolitics startups ecosystem

1st and 2nd quantum revolutions

first quantum revolution

manipulating groups of quantum particles photons, electrons and atoms interactions



transistors, lasers, fiber optics, GPS photovoltaic cells, atom clocks medical imaging, digital photography and video LEDs, LCD TV quantum dots

1947-*

second quantum revolution

manipulating superposition and entanglement and/or individual particles



quantum computing quantum telecommunications quantum cryptography quantum sensing (cc) Olivier Ezratty, 2021, 2023

end of Dennard scale in 2006



Table MM-7Device Architecture and Ground Rules Roadmap for Logic Devices.

Note: GxxMxx/Tx notation refers to Gxx: contacted gate pitch, Mxx: tightest metal pitch in nm, Tx: number of tiers. This notation illustrates the technology pitch scaling capability. On top of pitch scaling there are other elements such as cell height, number of stacked devices, DTCO constructs, 3D integration, etc. that define the target area scaling (gates/mm²).



Acronyms used in the table (in order of appearance): LGAA—lateral gate-all-around-device (GAA), CFET (Complementary Field Effect Transistor), 3DVLSI—fine-pitch 3D logic sequential integration.

quantum computing promise



solving intractable / exponential problems in **reasonable** time

typical exponential problems





T31

| $\partial W(\alpha t)$ | $\lambda^2 = \lambda^2 m(\alpha + \lambda)$ | |
|--|---|----|
| $i\hbar \frac{\partial \Psi(x,t)}{\partial t} = -$ | $-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial^2}+V(x)\Psi(x,t)$ | t) |
| đt | $2m \partial x^2$ | - |

solving Schrodinger's wave equation to simulate quantum matter

machine learning and deep learning

| $rac{\partial^2 u_1}{\partial x_1^2} + rac{\partial^2 u_2}{\partial x_2 \partial x_1} +$ | ${\partial^2 u_3\over\partial x_3\partial x_1}+$ | $\frac{\partial^2 u_1}{\partial x_1^2} + \frac{\partial^2 u_1}{\partial x_2^2}$ | $+rac{\partial^2 u_1}{\partial x_3^2}+f_1=0$ |
|---|--|---|---|
| $rac{\partial^2 u_1}{\partial x_1 \partial x_2} + rac{\partial^2 u_2}{\partial x_2^2} +$ | ${\partial^2 u_3\over\partial x_3\partial x_2}+$ | $\frac{\partial^2 u_2}{\partial x_1^2} + \frac{\partial^2 u_2}{\partial x_2^2}$ | $+rac{\partial^2 u_2}{\partial x_3^2}+f_2=0$ |
| $\frac{\partial^2 u_1}{\partial x_1 \partial x_3} + \frac{\partial^2 u_2}{\partial x_2 \partial x_3}$ | $+ {\partial^2 u_3\over\partial x_3^2} +$ | $\frac{\partial^2 u_3}{\partial x_1^2} + \frac{\partial^2 u_3}{\partial x_2^2}$ | $+rac{\partial^2 u_3}{\partial x_3^2}+f_3=0$ |

solving partial derivative equations



breaking asymmetric cryptography keys

quantum computing usage categories

research

operations



10

what is a qubit?

basic unit of quantum information

vector in a 2-dimension complex numbers Hilbert space



probabilities and Born normalization constraint



Bloch sphere representation with amplitude and phase

oresentation and phase



two-level state controllable quantum object

separable atom energy level

0)



electron or nucleus spin orientation



photon mode (polarization, number, frequency) N qubits handle the equivalent of **2^{N+1} real numbers** during computation

it benefits from **quantum parallelism** brought by superposition, engtanglement and interferences



layout of a 133-qubit processor from IBM

from computing to measurement



a new programming model

visual quantum circuits design



https://algassert.com/quirk

online open source tool to learn, program and emulate up to 16 « perfect » qubits

scripted Python code

```
# Initialize counting qubits
# in state |+>
for q in range(n_count):
    qc.h(q)
```

```
# And auxiliary register in state |1>
qc.x(3+n_count)
```

```
# Do inverse-QFT
qc.append(qft_dagger(n_count), range(n_count))
```

```
# Measure circuit
qc.measure(range(n_count), range(n_count))
qc.draw(fold=-1)  # -1 means 'do not fold'
```

IBM Qiskit, Google Cirq, Eviden Qaptiva

some key differences

$$\begin{split} f(\lambda x) &= \lambda f(x) \text{ for all } \lambda, x \in \mathbb{R} \\ f(x+y) &= f(x) + f(y) \text{ for all } x, y \in \mathbb{R} \\ \langle \Psi_1 | \Psi_2 \rangle &= \left[\overline{\alpha_1}, \overline{\beta_1} \right] \times \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \overline{\alpha_1} \alpha_2 + \overline{\beta_1} \beta_2 \\ |\Psi_2 \rangle \langle \Psi_1 | &= \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \times \left[\overline{\alpha_1}, \overline{\beta_1} \right] = \begin{bmatrix} \alpha_2 \overline{\alpha_1} & \alpha_2 \overline{\beta_1} \\ \beta_2 \overline{\alpha_1} & \beta_2 \overline{\beta_1} \end{bmatrix} \end{split}$$

need to understand linear algebra



breakpoints become endpoints

uncopiable data, but transferable

main qubit types



quantum & classical computing paradigms

| classica | l computers | analog quantu | m computers | digital quantur | m computers | |
|---|---|--|-----------------------------|--|---|------------|
| quantum inspired | quantum emulators | quantum | analog | gate-b | ased | |
| running on classical computer, inspired by quantum algorithms. | computers code on classical computers, for training, debugging and testing | annealing computers | quantum simulators | NISQ (Noisy Intermediate Scale Quantum) no error correction with a few noisy qubits | FTQC (Fault-Tolerant Quantum Computers) error correction and fault tolerance | y, 2023 |
| classical algorithms improvements | quantum algorithms debug and testing | optimization proble physics sin | ems and quantum mulation | general purpose qua adds search and in | antum computing, nteger factoring | ier Ezratt |
| | eviden <u>IEM</u> | | | IBM rigetti | Ψ PsiQuantum | (cc) Oliv |
| | FUJITSU Google | (, , , , , , , , , , , , , , , , , , , | | Google IQM | ALICE & BOB | |
| ZAPATA //AI | Microsoft aWS | | : 434 44 1 F 420 × | | Microsoft | |
| | QUANDELA C12 | | | QUANTINUUM QUANDELA XANAD | U | |

émulateur quantique (langa)

Domaine : INFORMATIQUE/Info Définition : Dispositif qui util conçu pour un ordinateur c Note : La durée d'exécution exponentiellement avec le superordinateurs classiques Voir aussi : algorithme quant Équivalent étranger : quantur



Mardi 20 décembre 2022/N° 294

SOMMAIRE ANALYTIQUE

LOIS

1 LOI nº 2022-1587 du 19 décembre 2022 visant à lutter contre la fraude au compte personnel de formation et à interdire le démarchage de ses titulaires

Décrets, arrêtés, circulaires

textes généraux

Première ministre

- 2 Arrêté du 4 novembre 2022 établissant la liste des membres du Conseil supérieur des gens de mer
- 3 Arrêté du 15 décembre 2022 relatif à l'approbation de la modification du cahier des charges de l'appel à projets « Innovations en biothérapies et bioproduction »
- 4 Avenant nr 2 du 19 décembre 2022 relatif à la convention du 13 février 2017 portant avenant nr 4 à la convention du 20 octobre 2010 entre l'Etat et l'Agence nationale pour la rénovation urbaine (ANRU) relative au programme d'investissements d'avenir (actions : « Internats d'excellence et égainté des chances » et « Internats de la réussite »).

ministère de l'économie, des finances et de la souveraineté industrielle et numérique

- 5 Arrêté du 2 décembre 2022 portant abrogation de l'arrêté du 21 octobre 2022 pris en application des articles L. 562-3 et suivants du code monétaire et financier
- 6 Arrêté du 13 décembre 2022 relatif à la classification des engagements d'assurance consécutifs aux atteintes aux systèmes d'information et de communication

uter un algorithme quantique

nulation quantique croissent npliquer le recours à des

quantum computing paradigms

gates-based quantum computers

quantum annealers

quantum simulators







sequential programming of quantum gates, can implement any algorithm and Hamiltonian transformation



QUANDELA

finding a ground state of an Ising model, optimization problems are mapped to Ising models (QUBO)



finding a ground state of an Ising model or XY quantum simulation model (with more degrees of liberty)



analog quantum computing



some mathematical **problem** with data inputs and desired output.

algorithm to solve the given problem, which are mostly hybrid and/or variational.

with analog quantum computing, the quantum part of the algorithm may map itself to a generic QUBO or Ising **model formulation.**

QUBO/Ising model may itself map to a generic problem formulation like **BQM** in the case of D-Wave annealers.

the reformulated problem is **directly solved** by the (analog) quantum computer, in an hybrid manner along with a classical computer.

QPUs vendors per qubit type







23

(cc) Olivier Ezratty, 2024

France QPU startups















inside a typical quantum computer



for superconducting or electron spin qubits

superconducting qubits





Harvard / QuEra logical qubits



source: Logical quantum processor based on reconfigurable atom arrays by Dolev Bluvstein, Mikhail D. Lukin et al, December 2023 (32 pages).

all qubit types have their challenges

quantum annealing

- mature development tools offering.
- large number of software startups, particularly in Japan and Canada.
- quantum annealers are available in the cloud by D-Wave and Amazon Web Services.
- · the greatest number of well documented case studies in many industries although still at the proof of concept stage.
- most universal oubits gates algorithms can be

superconducting qubits

- key technology in public research and with commercial vendors (IBM, Google, Rigetti,
- record of 433 programmable gubits with IBM.
- constant progress in noise reduction. could enable a record low ratio of physical/logical pubits.
- many existing enabling technologies:
- potentially scalable technology and

particularly with the cat-oubits variation which

- cryostats, cabling, amplifiers, logic, sensors.
- deployable in 2D geometries.

trapped ions qubits

- identical ions => no calibration required like with superconducting/electron spin aubits.
- good gubits stability.
- excellent gubit gate fidelities and high ratio between coherence time and gate time => supports deep algorithms in number of gate cycles.
- entanglement possible between all gubits on 1D
- requires some cryogeny at 4K to 10K => simpler.
- easy to entangle ions with photons for long distance communications.

silicon spin qubits

- good scalability potential to reach millions of gubits, thanks to their size of 100x100 nm.
- works at around 100 mK 1K => larger cooling
- relatively good oubits fidelity reaching 99.6% of gubits.
- adapted to 2D architectures usable with
- surface codes or color codes QEC.
- can leverage existing semiconductor fabs. good quantum gates speed.

- scalability remains to be demonstrated.

qubits NV centers

- works at 4K, with simple cryogeny without dilution
- can also potentially work at ambiant temperature, with some limitations on entanglement.
- long coherence time > 1 ms.
- strong and stable diamond structure.
- can also help create quantum memory for other qubits types, like superconducting qubits.
- · possible to integrate it with optical quantum telecommunications.

- manufacturing.

relatively slow computing due to long quantum gate times which may be problematic for deep algorithms.

neutral atoms qubits

- · long qubit coherence time and fast gates.
- operational systems with 100-300 atoms. identical atoms, that are controlled with the
- same laser and micro-wave frequencies (but
- works in both simulation and gate-based
- no need for specific integrated circuits.
- uses standard apparatus.
- low energy consumption.

- losing atoms during computing.

- **Majorana fermions**
- theorically very stable gubits with low level of required error correction.
- long coherence time and gates speed enabling processing complex and deep algorithms.
- potential gubits scalability, built with technologies close to electron spin qubits.
- field could be fruitful with no Maiorana

- no Maiorana fermion gubit demonstrated vet.

photons aubits

- stable gubits with absence of
- gubits processing at ambiant temperature. emerging nano-photonic manufacturing
- easier to scale-out with inter-oubits
- telecommunications.
- MBOC/FBOC circumventing the fixed gates depth computing capacity.

- not yet scalable in number of operations due to probabilistic character of quantum gates and the efficiency of photon sources in most paradigms.

gubit fidelities are average with most vendors.

key hardware challenges



qubits fidelities



errors mitigation and correction



(e) t type modularity involves microwave-to-optical transduction to link QPUs in different dilution refrigerators.

quantum interconnect



enabling technologies scalability



energy consumption



quantum memory

raw algorithm fidelities requirements



desired error rate $< \frac{1}{N \times D}$

| | | | required | | | |
|-----|--------|-------|------------|--------------|---------------|--|
| N D | | | error rate | required | available | |
| | qubits | depth | (%) | fidelity (%) | fidelity (%) | |
| | 50 | 100 | 0.02000% | 99.98% | 99.30% | |
| | 133 | 300 | 0.00251% | 99.9975% | 99.6% | |
| | 433 | 1000 | 0.00023% | 99.9998% | 98% | |
| | 1121 | 2000 | 0.00004% | 99.99996% | N/A | |

qubit errors quickly kills quantum computing accuracy



qubit errors sources



how to improve qubit fidelities? *



materials



manufacturing





tune qubit parameters

Cross-Cross Resonance Gate

Kentaro Heya^{1,2,*} and Naoki Kanazawa^{1,†}

¹ IBM Quantum, IBM Research Tokyo, 19-21 Nihonbashi Hakozaki-cho, Chuo-ku, Tokyo 103-8510, Japan ² Research Center for Advanced Science and Technology (RCAST), The University of Tokyo, Meguro-ku, Tokyo 153-8904, Japan

High-fidelity three-qubit iToffoli gate for fixed-frequency superconducting qubits

 Yosep Kim,^{1,*} Alexis Morvan,¹ Long B. Nguyen,¹ Ravi K. Naik,^{1,2} Christian Jünger,¹ Larry Chen,² John Mark Kreikebaum,^{2,3} David I. Santiago,^{1,2} and Irfan Siddiqi^{1,2,3}
 ¹Computational Research Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA
 ³Materials Science Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA (Dated: December 21 2022)

use different primary gates



improve control signals quality

logical qubits and FTQC

physical qubit

error rates ≈0.1%

logical qubit

error rate $<10^{-8}$ to $<10^{-15}$

error correction code

threshold, physical qubits overhead, connectivity requirements, syndrome decoding and scale

fault tolerance

avoid error propagation and amplification implement a universal gate set fault-tolerant results readout



tens to thousands qubits

Microsoft-Quantinuum logical qubits

Demonstration of logical qubits and repeated error correction with better-than-physical error rates

M. P. da Silva,¹ C. Ryan-Anderson,² J. M. Bello-Rivas,¹ A. Chernoguzov,² J. M. Dreiling,² C. Foltz,² J. P. Gaebler,² T. M. Gatterman,² D. Hayes,² N. Hewitt,² J. Johansen,² D. Lucchetti,² M. Mills,² S. A. Moses,² B. Neyenhuis,² A. Paz,¹ J. Pino,² P. Siegfried,² J. Strabley,² S. J. Wernli,¹ R. P. Stutz,² and K. M. Svore¹

¹Microsoft Azure Quantum ²Quantinuum (Dated: April 2, 2024)

The promise of quantum computers hinges on the ability to scale to large system sizes, e.g., to run quantum computations consisting of more than 100 million operations fault-tolerantly. This in turn requires suppressing errors to levels inversely proportional to the size of the computation. As a step towards this ambitious goal, we present experiments on a trapped-ion QCCD processor where, through the use of fault-tolerant encoding and error correction, we are able to suppress logical error rates to levels below the physical error rates. In particular, we entangled logical qubit states encoded in the [[7, 1, 3]] code with error rates 9.8× to 500× lower than at the physical level, and entangled logical qubit states encoded in a [[12, 2, 4]] code with error rates below physical circuit baselines corresponding to repeated CNOTs, and show evidence that the error rate of two physical CNOTs. These results signify an important transition from noisy intermediate scale quantum computing to reliable quantum computing, and demonstrate advanced capabilities toward large-scale fault-tolerant quantum computing.

https://arxiv.org/abs/2404.02280

claim: logical qubit with x800 improvement vs physical qubit reality: x800 improvement only for the first gate cycle!



FIG. 7. Observed error rate for circuits with 1 to 3 rounds of error correction with the [[12, 2, 4]] Carbon code (green circles) and physical baselines (blue diamond for pairs of 1bit teleportations, and orange squares for pairs of CNOTs). Results are offset along the x-axis for clarity. Linear fits are obtained by maximum-likelihood estimation (see Appendix A for details).

https://scottaaronson.blog/?p=7916#comment-1973425

logical qubits requirements



NISQ VQA process

VQE for benzene ground state 72 qubits and 330,816 Pauli strings





number of physical qubits

key software challenges



data loading



tensor networks competition



actual speedups



benchmarking



actual computing time



coding abstraction level

quantum algorithms patterns









« hidden » function used in search algorithms, may rely on quantum memory



amplitude amplification used in Grover algorithm



uncompute trick

to disentangle ancilla qubit after computing without losing results, used in HHL, U being a QPE



measurement

with optional basis change using Pauli strings (in VQA)



data preparation other algorithms

or

period finding finds the periods decomposes or recomposes a of a signal signal into/from it components creates a superposition of 2st computational states controlled U operation and phase kickback to inverse quantum Fourier transform first n aubit 0) — H unitary U 7 0) — H QFT any combination $|0\rangle - H$ $C - U^{2^0} - C - U^{2^1} - \cdots - C - U^{2^{n-1}}$ of quantum gates $|\psi\rangle \neq^m$ epeated $O(1/\epsilon)$ times

QFT

phase

estimate

(QPE)



ansatz

Hamiltonian injection used in NISQ variational algorithms

algorithms inputs and outputs

| | algorithm | classical input | quantum input blue for superposed state | quantum output blue for superposed state | classical output | acceleration (# of circuit runs) |
|------|--------------------|--|---|---|---|--|
| | Deutsche-Jozsa | balanced or unbalanced function in oracle | oracle function | function is balanced if all output qubits are at ground state $\left 0\right\rangle$ | « yes or no » | exponential (O(1)) |
| | Bernstein-Vazirani | string encoded in a function | can be entirely quantum using a series | (integer) secret string in basis encoding | integer | exponential (O(1)) |
| | Grover | function returning 1 only for one basis | use case) or access some classical data in superposition using a qRAM (which | searched item index as integer in basis encoding | integer | quadratic (O(1)) |
| ž | Simon | periodic function | does not exist yet) | parameters for a linear equation used to find a period, with average of basis encoding | integer representing function period | exponential (O(1)) |
| Ē | Shor factoring | semi-prime integer | Hadamard gates and parametrized period finding function with | regularly spaced amplitudes starting with 0 | dividing integer found with continuous fraction post- | exponential (depends period |
| | Shor dlog | two integers | exponentiations | | processing | finding integer) |
| | QFT | series of values | series of complex amplitudes with | Fourier coefficients in amplitude encoding, enabling the recovery of the main frequency | main frequency | exponential (O(1)) |
| | QPE | Hamiltonian | amplitude encoding | phase encoded in bitstring | phase as a real number | exponential (O(1)) |
| | HHL | one vector and one matrix | one vector and one matrix amplitude encoding | inverted matrix x entry vector (= one vector) in amplitude encoding | characteristics of the vector to obtain one eigenvalue | exponential (depends) |
| | QAOA | objective function to optimize | cost function parameters aneoded in | probabilistic distribution of Pauli strings | cost function value and objective function params | not proven (many) |
| NISQ | VQE | problem Hamiltonian | an ansatz function (rotation gates and CNOTs) | probabilistic distribution of Pauli strings components of Hamiltonian ground state | cost function evaluation, ansatz update, ground state Hamiltonian | not proven (many due to cost function convergence, Pauli strings # & precision) |
| | QML classification | depends (training, inference, model) | object vector to classify encoded in amplitude | prediction result as an integer index in basis encoding | integer representing object position in a reference table | depends (many) |

potential quantum speedups



a matter of perspective



(cc) Olivier Ezratty, 2023, inspired by Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage by Torsten Hoefler, Thomas Häner, Matthias Troyer, 2023.

quantum advantages taxonomy







€\$£ TCO ROI

space

the qubit register data space - scaling in 2^N complex numbers with N qubits - exceeds the memory capacity of classical computers.

speed

a quantum algorithm, including its classical part, runs faster than an equivalent best-inclass classical algorithms running on either the largest supercomputers or a given HPC configuration.

quality

the quality of the results of a quantum algorithm is better for some respect than the best-in-class classical algorithms. e.g: an error rate of a machine learning classification, a chemical simulation accuracy, or a better combinatorial problem solution.

energetic

a fully-burdened quantum computer and algorithm configuration consumes less energy than the best-in-class classical equivalent.

cost

the total cost of the quantum solution is lower than the total cost of a best-inclass classical solution.

a long journey



quantum computing cloud offerings



what is being practically done

| classical computers | | analog quantum computers digital quantum comp | | n computers | |
|--|---|--|--|---|---|
| quantum inspired | quantum emulators | quantum annealing computers | analog quantum simulators | gate-ba NISQ (Noisy Intermediate Scale Quantum) | FTQC (Fault-Tolerant Quantum Computing) |
| financial services solutions improvements. machine learning improvements. | code learning. code debugging. designing new algorithms. simulating qubit physics. simulating error correction codes. | solving optimization problems at mid- sized scale, in transportation (Volkswagen, Denso), retail (Ocado, Pattison), job shop scheduling and financial services (Mastercard, CACIB). physics simulations (statistical physics, spin glass, ferromagnetism, topological matter,). potential energetic advantage. | | low-level physics simulations ("IBM quantum utility" with 127 qubits and kicked Ising model). creating and testing algorithms at small scale (QML, optimizations, chemical simulations). | large algorithms and resource estimations. creating and testing error correction codes (Google, Quantinuum, QuEra, PsiQuantum,). |
| CALPHARAIL | Qubit I | CaixaBank Raiffeisen Bank International Member of RBI Group | CRÉDIT AGRICOLE CORPORATE & INVESTMENT BANK | AIRBUS EDF MBDA ISSUE SUBTER | B HYUNDRI J.P.Morgan Goldman Sachs |

why study quantum computing now?

- **1. understand** the quantum computing technology and buzz.
- 2. **become ready** when quantum computing delivers.
- **3.** attract **high-level talent** in your organization.
- 4. challenge and revisit legacy classical solutions.
- 5. envision lower energy consumption in HPC applications.



industry vendors ecosystem





discussion