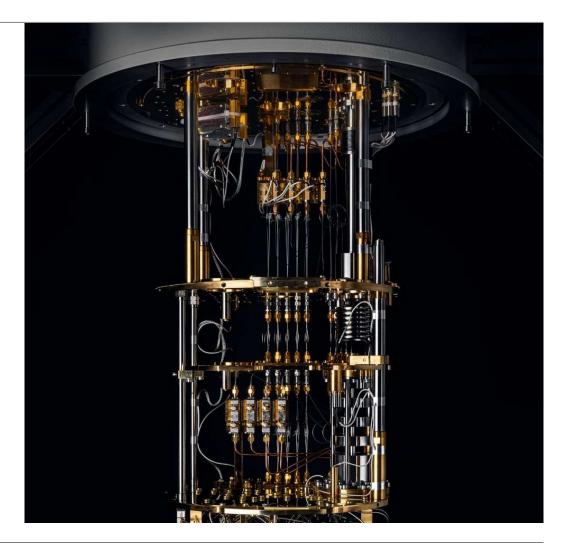
WE BUILD QUANTUM COMPUTERS

Introduction to Quantum Computing and its Applications



Dr. Mikio Nakahara

IQM Quantum Computers

www.meetiqm.com

We Build Quantum Computers

IQM

IQM builds and
285+
delivers
quantum
computersExperts
the bigg
quantum
in Euro
the wor
On-pre

Experts one of the biggest quantum teams in Europe and the world.

On-premises & full access

3 systems sold and delivered to

2 systems sold and delivered to



Spark sold to Julich SC





Full-stack solutions with **co-design**

Own facilities \rightarrow fast turnaround

IQM's Private Foundry: 600 m2

200M€+ funding





Council

Fast Lane to Quantum Advantage

We build world leading

now and for the future.

quantum computers for the well-being of humankind,

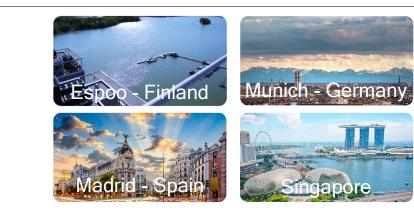
OUR MISSION



IQM builds and delivers quantum computers

OUR MISSION

We build world leading quantum computers for the well-being of humankind, now and for the future. 285+ experts 125+ PhDs 46+ nationalities





Palo Alto - USA

200M€ investment

On-premises & full access



IQM Product and Service Portfolio



On-premise / Product delivery

IQM Spark[™]

- quantum computer for research and education
- 5 or 20 tunable superconducting qubits with tunable couplers
- Hardware/Software access
- Fast delivery and affordable pricing



On-premise / Product delivery IQM Radiance™

- State-of-the-art on-premise offering
- Up to 150 qubits
- Integration-layer to HPC centres



Service provider

- IQM Resonance cloud offering
- IQM Academy
- Quantum education



Part I Overview

• Part II Near Term Quantum: Portfolio Optimization

Before we start our journey

- 1. Quantum computing will play more and more important roles in our society.
- 2. The unit of quantum information is **qubit** instead of **bit**.
- 3. The fundamental physics of our universe is quantum physics and relativity. The world we see is just a classical limit of these theories.
- 4. We don't see quantum phenomena in everyday life since it manifests itself only in a microscopic scale. But note that we doesn't exist without quantum theory. Our universe would not be created without quantum theory.
- 5. In contrast, we use relativity everyday through GPS and cellphone.

Outline

• Warm Up

- Foundations: Qubits, gates and superposition
- Quantum computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

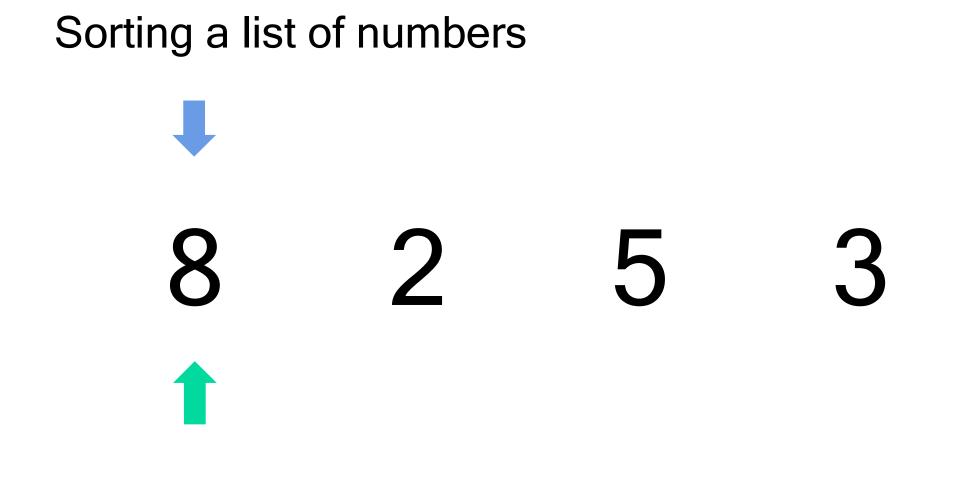
IQM

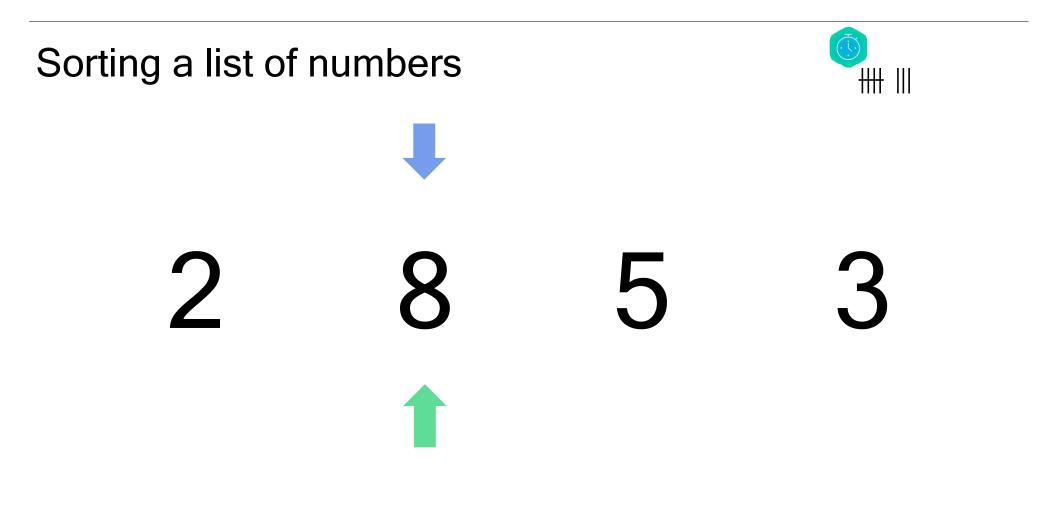


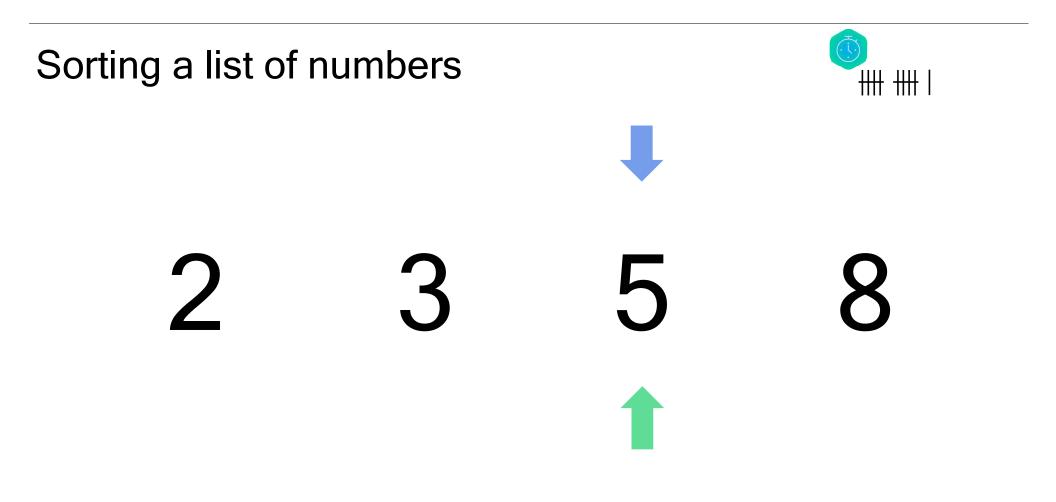
Warmup: Sorting a list of numbers

Conventional Algorithm

- 1. Suppose *n* positive numbers are given. Sort them in increasing order.
- 2. Find the smallest number and put it the left end.
- 3. Find the smallest number in the rest and put it next to the smallest number.
- 4. Repeat it until all numbers are exhausted.
- 5. This takes $O(n^2)$ steps.









Take-Home Message

- 1. Our spaghetti computer can sort n numbers in O(n) steps. n steps to cut, 2 steps to grab and press them against a table. Pick up one by one takes n steps, hence 2n + 2 steps.
- 2. Spaghetti computer is more efficient than digital computer. $O(n^2) \gg O(n)$ for $n \gg 1$.
- 3. How many steps it will take (computational complexity) depends on the resource you use. Quantum computer employes quantum system for computation.

Physics for Information Processing: Mechanical m-mail

https://www.miraikan.jst.go.jp/exhibitions/future/internet/

A white ball represents 0 while a black ball 1.

We Build Quantum Computers

There are problems a classical computer cannot (efficiently) solve

Problem with current computers:

- Intractable problems
- Fundamental limits
- Time & power limits

Current approach is not scalable!

"Latest findings suggest global computing is more likely responsible for between 2.1% and 3.9% of greenhouse gas emissions."

21=3*7; easy gas emissions." 109662352080961222027=52529305799*2087641373; harder

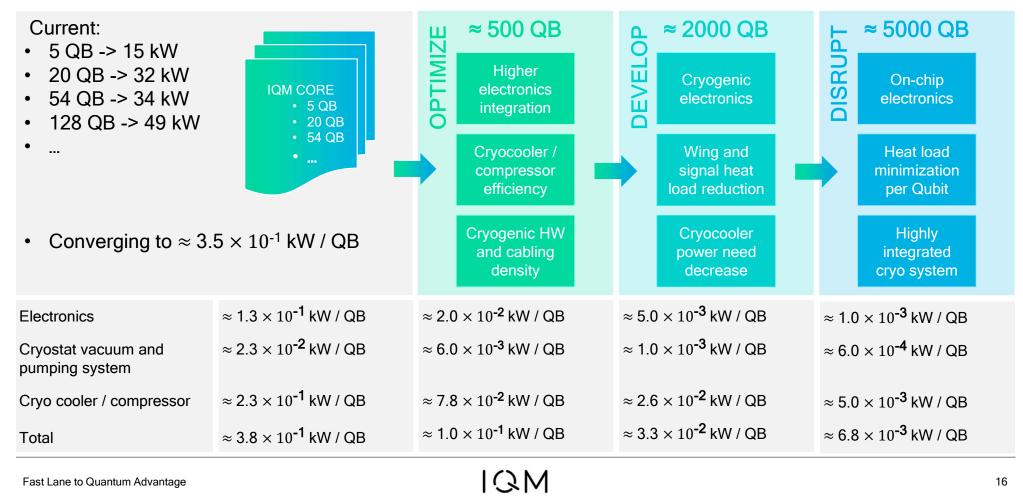
Fast Lane to Quantum Advantage

IQM

https://www.upi.com/Science News/2021/09/10/communications-techcarbon-emissions/8771631295350/

15

Quantum Sustainability



Outline

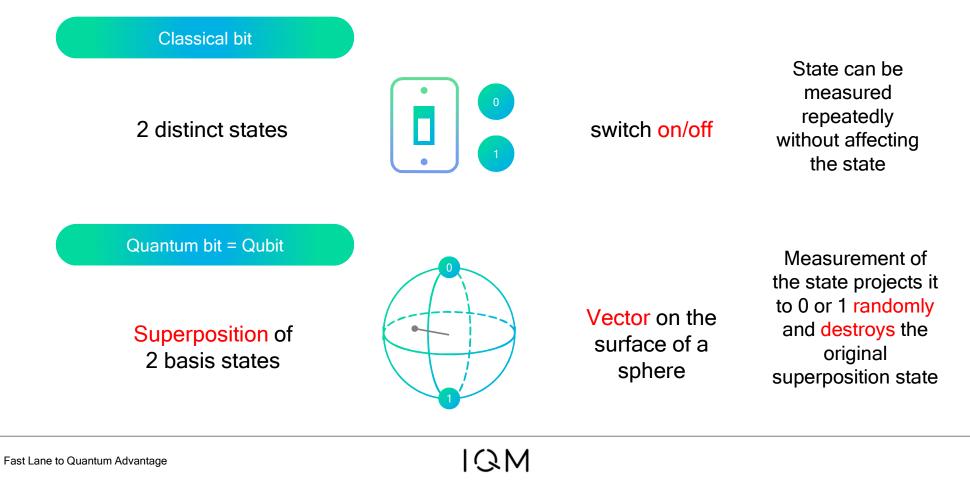
• Warm Up

- Foundations: Qubits, gates and superposition
- Quantum computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

IQM



Classical Computer vs. Quantum Computer



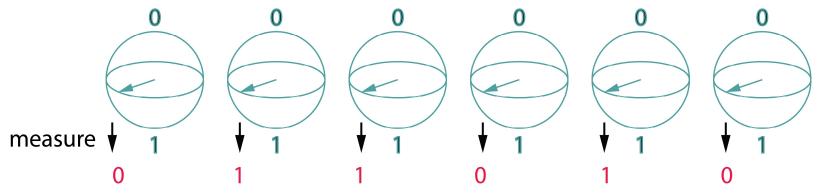
Classical Computer vs. Quantum Computer

- Measurement of a quantum state projects it to 0 or 1 randomly and destroys the original superposition state.
- If someone measures a qubit before you, the state will change to 0 or 1 when you measure it.
- Eavesdropping is detectable.
- Quantum key distribution (distributes classical encryption key securely: BB84). Already commercialized.

https://events.geant.org/event/453/contributions/436/attachments/273/408/2021-03-17_GEANT_Summary_Toshiba.pdf

Classical Computer vs. Quantum Computer

• Measurement of the state projects it to 0 or 1 randomly and destroys the original superposition state. Quantum random number generator.



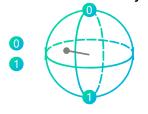
- Most random number generators currently available are "pseudorandom number generators" based on some algorithm, potentially hackable.
- Quantum random number generator is already commercialized.

Classical computer vs. Quantum computer

Quantum computers follow the rules of quantum physics.

Bit vs. Qubit (quantum bit)

A bit can be either 0 or 1, while a qubit can be in a superposition: qubit can be both 0 and 1 simultaneously. Measurement will yield either 0 or 1.



Two qubits can be **entangled**. Measuring one directly impacts the other.



Fast Lane to Quantum Advantage



→ 1 qubit can be in a superposition of 2 basis states → A 1 bit state can be just one out them

Basis states:

- 0
- 1

Classical computer vs. Quantum computer

Quantum computers follow different rules than classical computers - those of quantum physics.

Bit vs. Qubit (quantum bit)

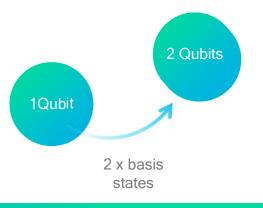
A bit can be either 0 or 1, while a qubit can be in a superposition: qubit can be both 0 and 1 at the same time. Measurement will yield either 0 or 1.

Two qubits can be entangled. Changing one directly impacts the other.



→ 2 qubits can be in a
superposition of all 4 basis states
→ A 2-bit state can be just one

out them



Basis states:

- 00
- 01
- 10
- 11



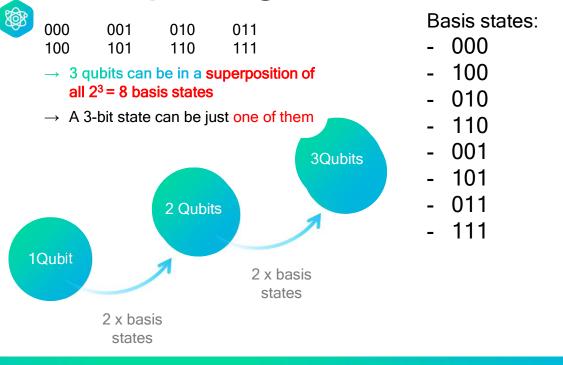
Classical computer vs. Quantum computer

Quantum computers follow different rules than classical computers - those of quantum physics.

Bit vs. Qubit (quantum bit)

A bit can be either 0 or 1, while a qubit can be in a superposition: qubit can be both 0 and 1 at the same time. Measurement will yield either 0 or 1.

Two qubits can be entangled. Changing one directly impacts the other.



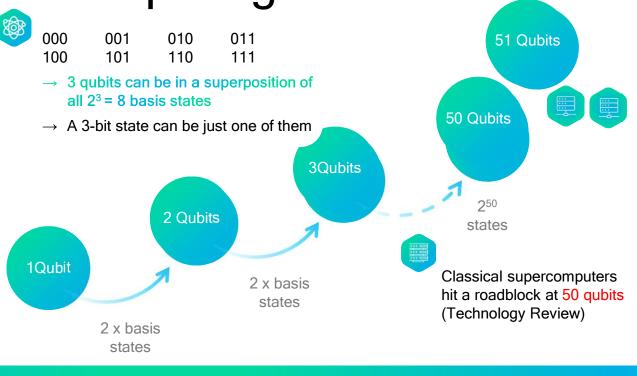
Classical computer vs. Quantum computer

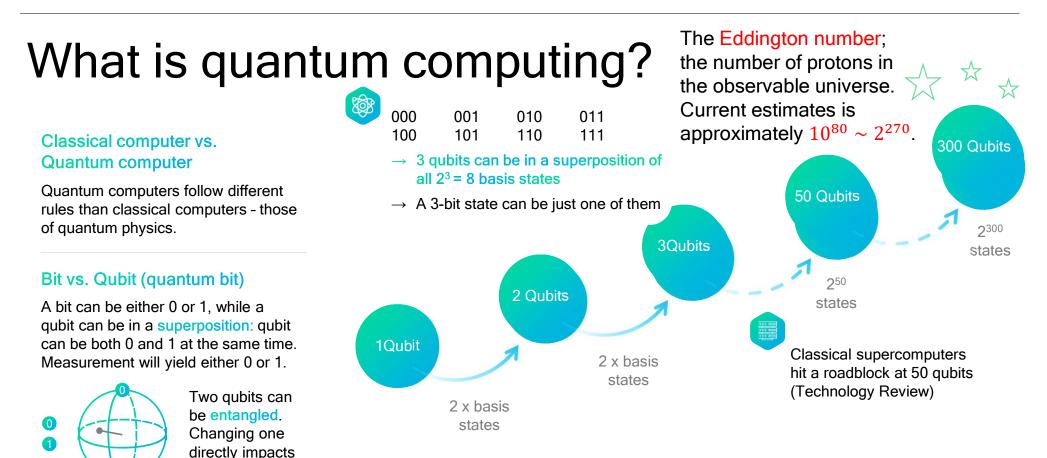
Quantum computers follow different rules than classical computers - those of quantum physics.

Bit vs. Qubit (quantum bit)

A bit can be either 0 or 1, while a qubit can be in a superposition: qubit can be both 0 and 1 at the same time. Measurement will yield either 0 or 1.

Two qubits can be entangled. Changing one directly impacts the other.





→ Exponential increase in computational capacity

 \rightarrow Enables new algorithms and solutions to previously intractable problems

Fast Lane to Quantum Advantage

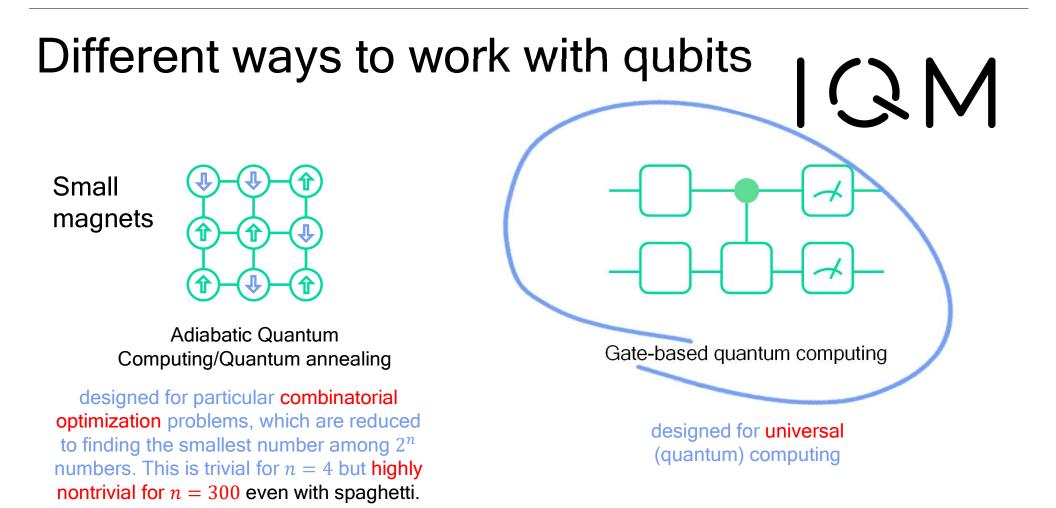
the other.

IQM

But how to work with those qubits?



IQM



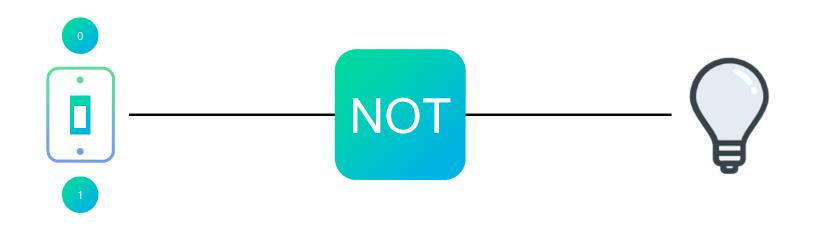
Conventional computer: bits

• Bits are the foundation of conventional computers



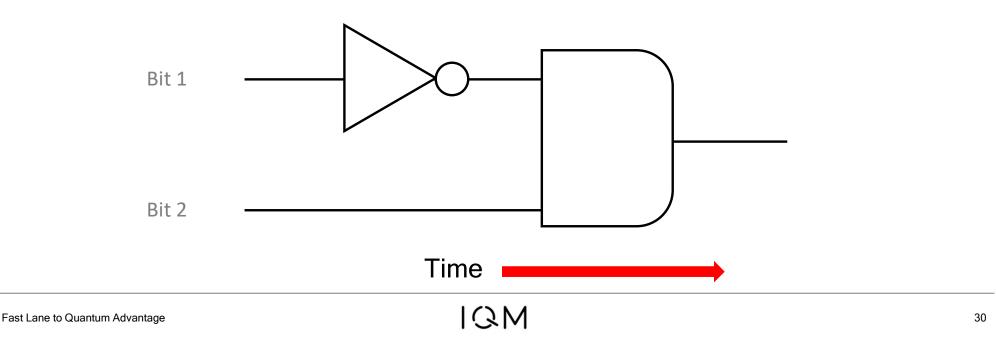
Conventional computer: working with bits

• Information processing is performed with the help of logical gates

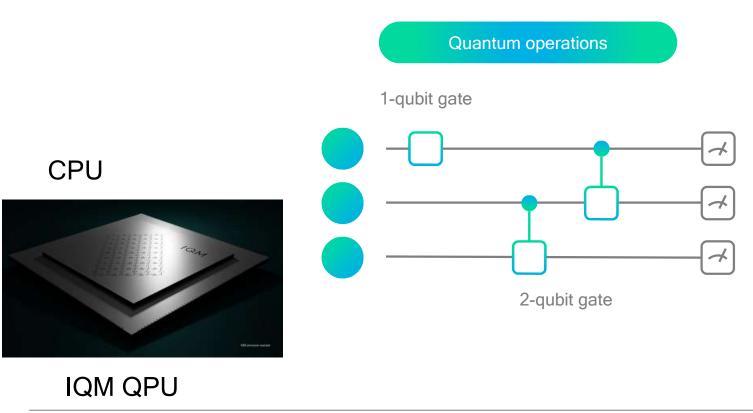


Conventional computer: algorithms

- Multiple gates form a (logical) circuit
- An <u>algorithm</u> is implemented in a sequence of gates
- Circuits are represented as a time sequence like musical score. A gate is a note.

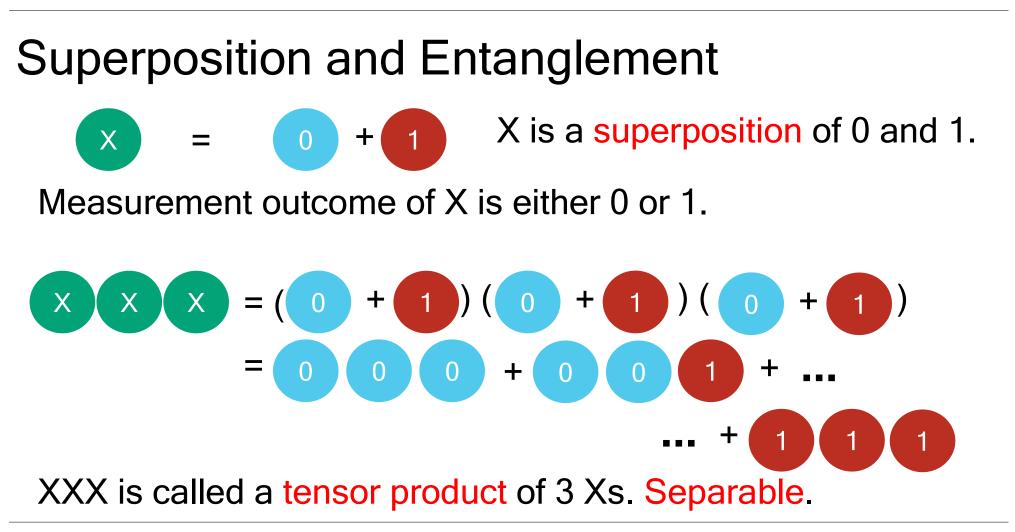


Quantum computers: algorithms



Universality Theorem: Any quantum algorithm can be decomposed into 1and 2-qubit gates

Quantum computing is reversible. Does not produce heat, does not require power. Power is required only for control electronics and refrigerator. (~ 30kW)



Superposition and Entanglement

 $\mathbf{0}$ If the first qubit is measured

?

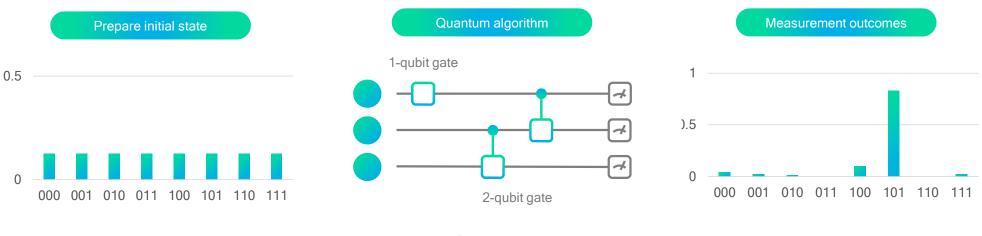
- and 0 is obtained, the second qubit is also 0.
- If the first qubit is measured and 1 is obtained, the second qubit is also 1.

0 $\left(\right)$ Andromeda Our ? Galaxy Galaxy

There are QKDs that make use of entangled states (E91, BBM92). Eavesdropping changes an entangled state to a product state.

╋

Quantum computing: algorithms

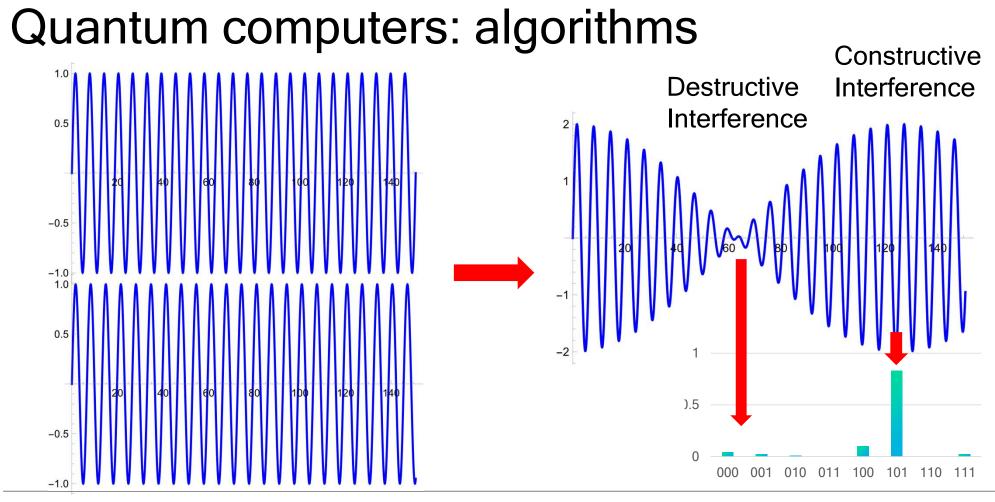


Prepare initial quantum state

Use interference to make wanted outcomes more likely

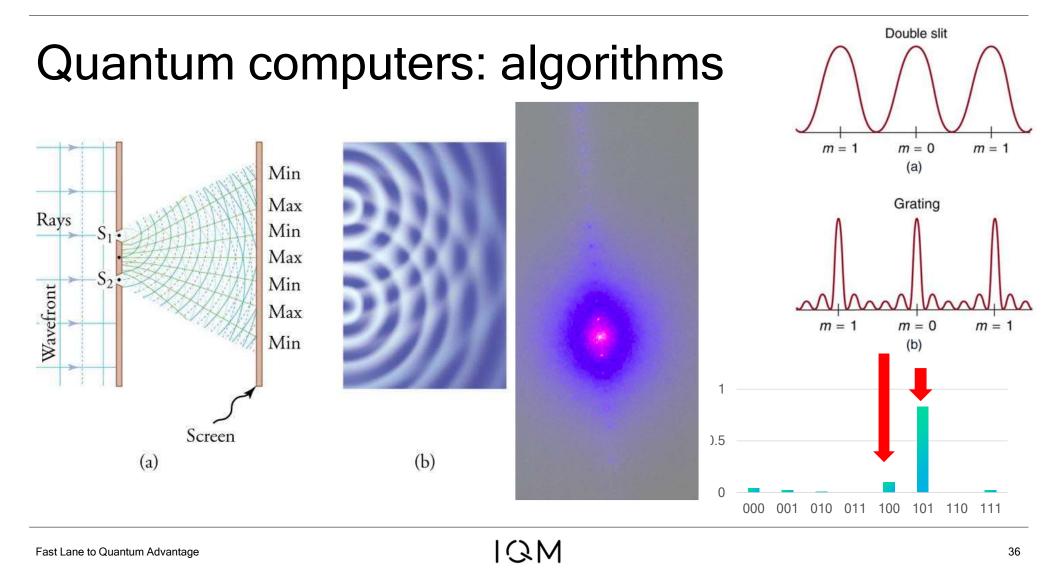
Measure multiple times

If the initial state is a superposition of 2^n states, the quantum circuit acts on 2^n states simultaneously! Quantum parallelism. $2^{270} \simeq 10^{80}$!



Fast Lane to Quantum Advantage

IQM



Quantum computers: algorithms

- Quantum algorithms leverage superposition and entanglement to enable new algorithms and manipulate qubits via quantum gates.
- Quantum algorithms explore a superposition of solution paths simultaneously. Quantum parallelism.
- Quantum algorithms use interference to amplify the likelihood of correct solutions to be measured, without knowing the solutions in advance.

).5

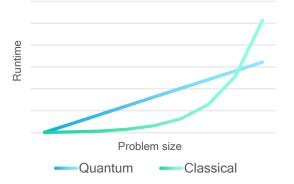
0

001

000



Quantum algorithms can provide up to **exponential speedup** for certain tasks in domains like simulation, optimization and machine learning.



Quantum computers do not speed up existing algorithms but allow new types of algorithms

Fast Lane to Quantum Advantage

1-qubit gate

Quantum operations

2-qubit gate

010 011 100 101 110 111

Measurement outcomes

Take-Home Message

- Unit of quantum information is qubit, which is a vector. As such, a qubit can be a superposition of 0 and 1.
- Multiple qubits can be entangled, which is not decomposable into a product of single qubit states. Separable states, which have classical analogue, are tiny, tiny fraction of qubit states. QC makes use of entangled states, which gives exponentially powerful computational power compered to its classical counterpart.
- Quantum algorithms are represented in terms of quantum circuits (quantum music score) by which the likelihood of the target state being measured is enhanced by interference.

VARTIAINEN et al.

PHYSICAL REVIEW A 70, 012319 (2004)

Quantum circuit to decompose 21 into 3 and 7. From J J Vartieinen, A O Niskanen, M Nakahara and M M Salomaa, Phys. Rev. A 70, 012319 (2004).

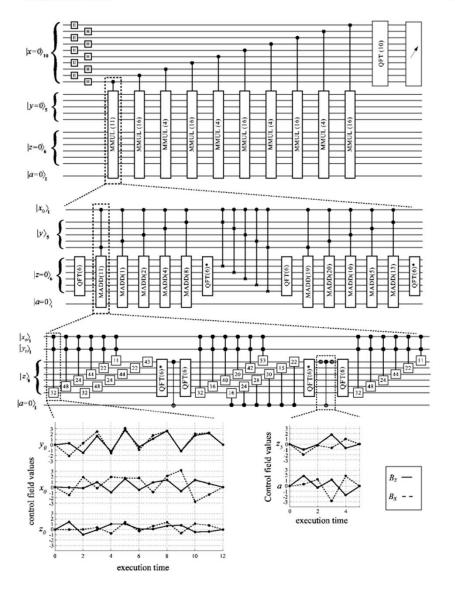


FIG. 5. Quantum circuit for Shor's algorithm factoring the number 21 with the parameter value a=11. The full circuit is shown topmost and the decompositions of the modular multiplier and adder blocks are indicated with dashed lines. The gates in the circuit have their conventional meanings, except that we denote a phase-shift gate by a box with a single number ϕ in it meaning that the phase of the state $|1\rangle$ is shifted by $e^{2\pi i \phi/2^n}$ with respect to the state |0>. Two examples of numerically optimized parameter sequences are also shown.

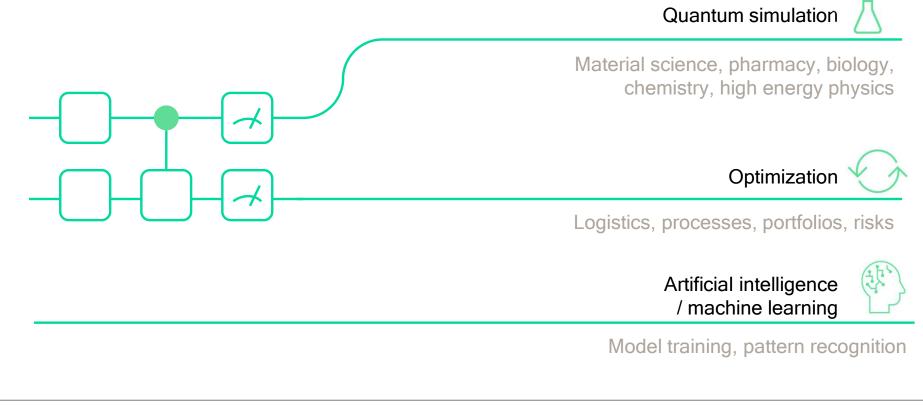
Outline

- Getting started
- Foundations: Qubits, gates and superposition
- Quantum computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

IQM



Quantum computing applications encompass three areas



Use-cases across sectors

Healthcare

- Drug discovery, Simulation of molecular interactions
- Improved diagnostics on small data
- Catalyst & enzyme design
- Personalized medicine
- ...

Brvironment

- Climate simulation
- Solar power capture
- Carbon capture
- ...



- Advertisement optimization
- Improved search
- ...



- Power grid optimization
- Energy distribution & demand management
- Demand forecasting
- Wind energy simulation

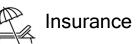
• ...



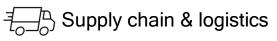
- Near-real-time risk assessment
- Portfolio optimization
- Derivative pricing

...

• ...



- Rating premium
- Risk analysis



- Supply chain & logistics optimization
- Capacitated vehicle routing
- Optimized itineraries
- ...

Industrial goods

- Development of materials (e.g. Aerospace)
- Optimization of industrial designs (chips, sensors on car, ...)
- ...

Retail

- Recommender systems
- Dynamic pricing
- ...

QUANTUM COMPUTING EXPO TOKYO Participants (2022)

https://www.nextech-week.jp/hub/en-gb/exhibit/qc.html

QUANTUM COMPUTING EXPO TOKYO Participants (2023)

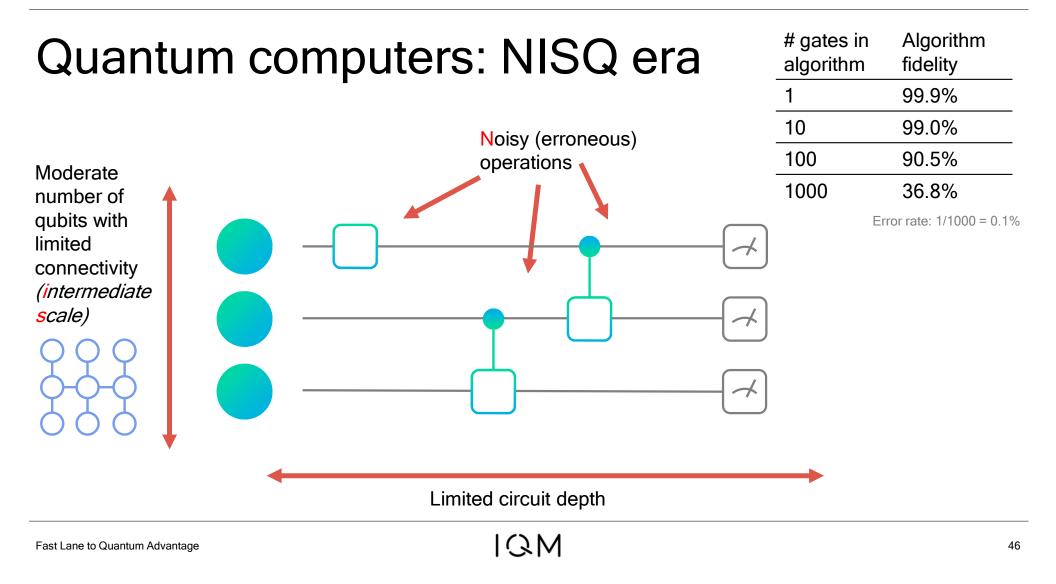
https://www.nextech-week.jp/hub/ja-jp/exhibit/qc.html

Outline

- Getting started
- Foundations: Qubits, gates and superposition
- Quantum computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

IQM



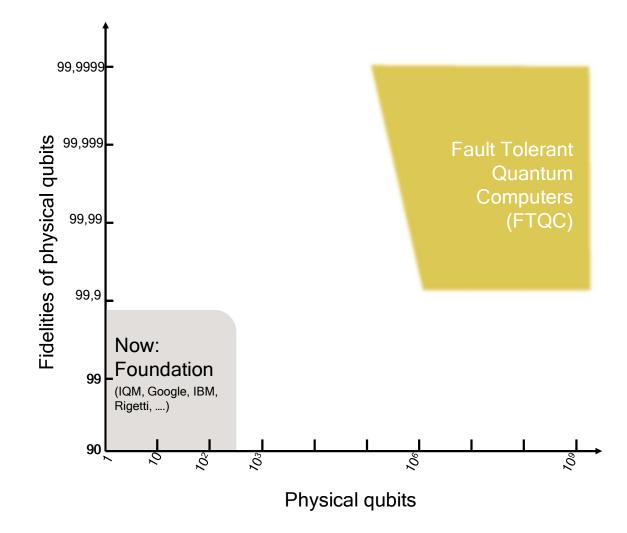


NISQ and FTQC

• Horizon: Fault Tolerant (FT) area

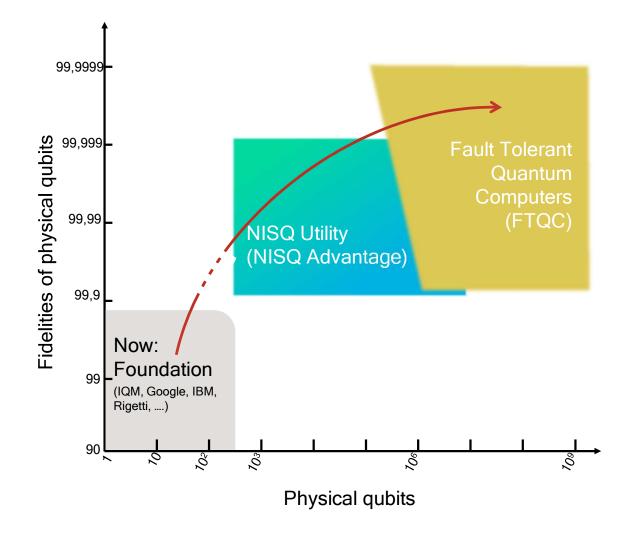
Why so complex?

- Error correction is based on redundancy
- 1 single fault tolerant logical qubit requires multiple physical qubits
- Noise needs to be reduced below a certain threshold



NISQ and FTQC

- Horizon: Fault Tolerant (FT) area
- But before that: Blue region (NISQ Advantage)
 - o Hybrid approaches
 - Potential for NISQ quantum utility



Quantum Computing Is Becoming Business Ready (Boston Consulting Group)

https://www.bcg.com/publications/2023/enterprise-grade-quantum-computing-almost-ready

What can fault-tolerant quantum computer do?

- Prime number factorization cannot be done in polynomial time classically. It takes exponentially long time to factor $N = p \times q$.
- It takes billions of years to decompose a large *N*. This fact is utilized in the RSA cryptosystem. We can do internet shopping safely thanks to this.
- Shor's algorithm can factor a large composite number quantum mechanically in reasonable time.
- Fortunately, the algorithm requires a large number of qubits and FT gates, which is beyond the currently available NISQ QC.
- Are we safe for the time being? No! "Store now, decrypt later (SNDL)" attack.
- Post-Quantum Cryptography (PQC) is an active field of research. <u>https://en.wikipedia.org/wiki/NIST Post-Quantum Cryptography Standardization</u> <u>https://csrc.nist.gov/Events/2024/fifth-pgc-standardization-conference</u>

Outline

- Getting started
- Foundations: Qubits, gates and superposition
- Quantum Computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

IQM



IQM: Unlocking early industry applications with the unique co-design approach

One-of-a-kind approach to industry applications

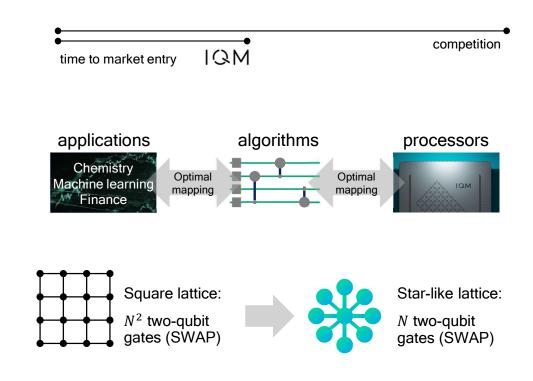
 Hardware efficiency through application-specific solutions (QuASICs) using a unique Co-Design approach

Faster time-to-market for industry applications

- Less qubits required compared to general-purpose approach
- Fewer gates required compared to general-purpose approach

Example: Algorithm for improving NMR imaging

- Adopted chip geometry to reduce hardware overhead
- \rightarrow Better gate efficiency by using a star-shape chip geometry



Take-Home Message

- Full-fledged fault-tolerant QC is still beyond our reach.
- QC currently available is a NISQ (Noisy Intermediate-Scale Quantum) computer. There are many useful algorithms when it is combined with classical computer. Simulation of physical systems, optimization, machine learning etc.
- FT QC is expected to crack codes. Post Quantum Cryptography is an active area of research to fight against "store now, decrypt later" attack.
- QC produces enormous amount of business opportunities. Potential of \$10-100B for each use case.
- IQM offers on-premises quantum computer while most vendors offer cloud services. On-premises quantum computer is mandatory when security must be guaranteed.

Outline

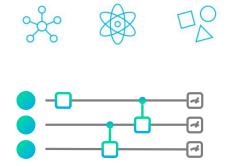
- Getting started
- Foundations: Qubits, gates and superposition
- Quantum Computing applications
- Current era of quantum computing
- IQM's approach to quantum computing
- Conclusion

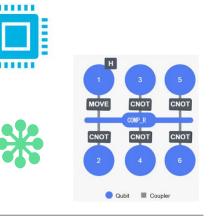
IQM



Conclusion

- Quantum computing can solve problems where conventional computers reach limits
- This requires clever algorithms that make optimal use of quantum properties of qubits
- Currently there are challenges to overcome; however, early adopters are prime to profit the most
- Co-Designing QuASICS as a mean to reducing the time to early industry applications





Recommended books

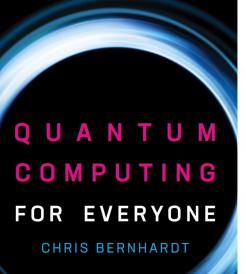
Quantum Computation and Quantum Information

MICHAEL A. NIELSEN and ISAAC L. CHUANG CRC Press Taylor & Francis Group A TAYLOR & FRANCIS BOOK

QUANTUM COMPUTING From Linear Algebra

to Physical Realizations





O'REILLY" Programming Quantum Couputers Essential Algorithms and Code Samples

Eric R. Johnston, Nic Harrigan & Mercedes Gimeno-Segovia

Fast Lane to Quantum Advantage

CAMBRIDG



WE BUILD QUANTUM COMPUTERS

Part II Quantum algorithms in the NISQ era: Portfolio Optimization (slightly more technical)

Dr. Mikio Nakahara

Quantum Education Manager, IQM

www.meetiqm.com



Outline

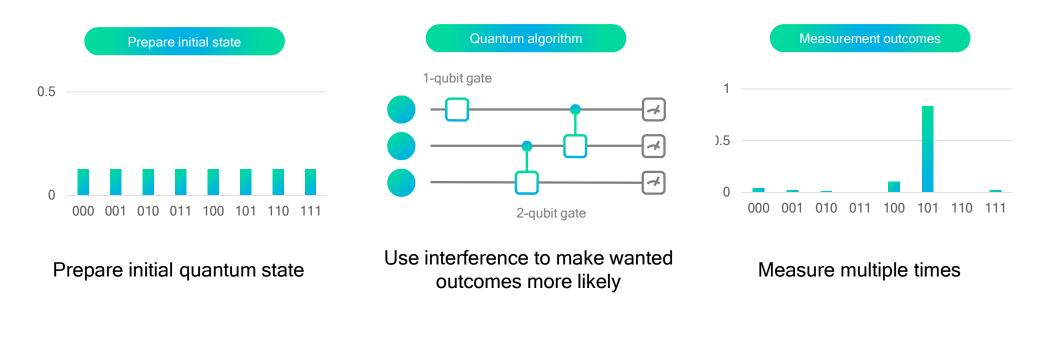
 Practical applications with quantum algorithms: algorithms for the NISQ era



Fast Lane to Quantum Advantage

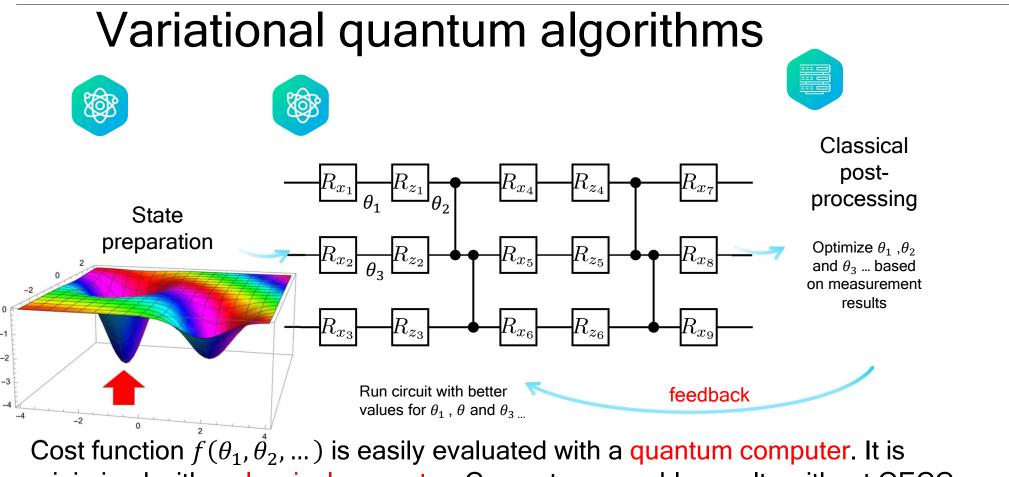
IQM

Quantum Algorithms, recap.



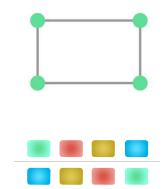
Near-term quantum algorithms

- They should solve useful problems
- They should require a moderate number of qubits
- They should work without error correction
- The circuit depth should be moderate

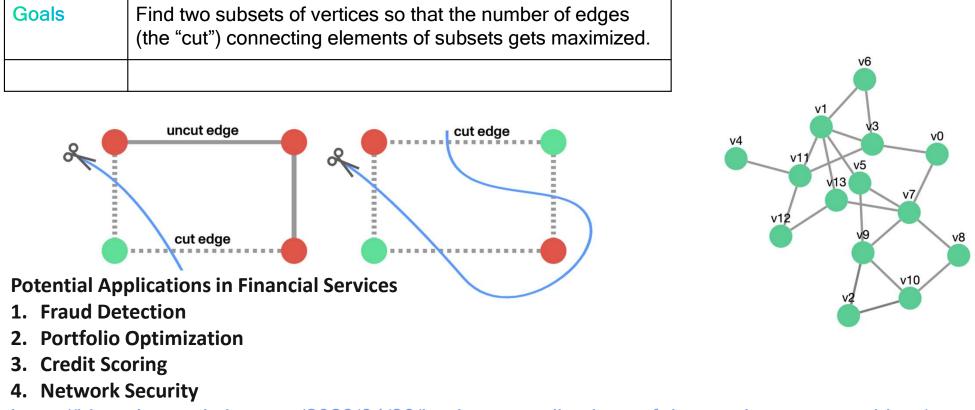


minimized with a classical computer. Can get reasonable results without QECC.

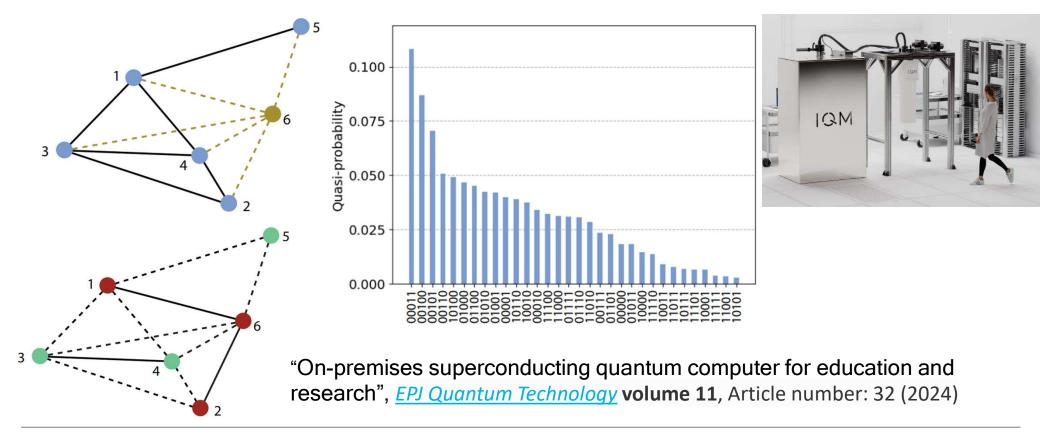
- Heuristic algorithm designed to find approximate solutions for combinatorial optimization problems
- Potential to be used to solve a wide range of combinatorial optimization problems, including:
 - Minimization: cost, distance, length of a traversal, weight, processing time, material, energy consumption, number of objects
 - Graph problems, such as finding best paths to travel
 - Scheduling problems, such as scheduling a set of jobs on a set of machines
 - Financial problems, such as portfolio optimization
 - Maximization: profit, value, output, return, yield, utility, efficiency, capacity, number of objects





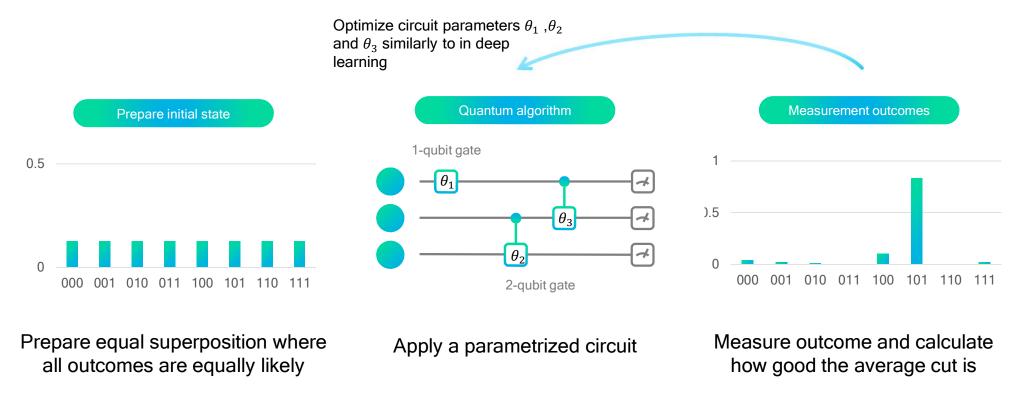


https://blog.algoanalytics.com/2023/04/20/business-applications-of-the-maximum-cut-problem/



Fast Lane to Quantum Advantage

IQM



- Many optimization problems are reduced to find the lowest energy state of a type of magnet (Ising Model). Find the smallest element of a diagonal matrix.
 - 1. Partitioning Problems
 - <u>Number Partition</u>
 - Graph Partition
 - Cliques
 - Reducing N to $\log N$ Spins in Some Constraints
 - 2. Binary Integer Linear Programming
 - 3. Covering and Packing Problems
 - Exact Cover
 - Set Packing
 - Vector Cover
 - Satisfiability
 - Minimal Maximal Matching
 - 4. Problems with Inequalities
 - Set Cover
 - Knapsack with Integer Weights
- Fast Lane to Quantum Advantage

- 5. Coloring Problems
 - Graph Coloring
 - Clique Cover
 - Job Sequencing with Integer Lengths
 - 6. Hamiltonian Cycles
 - Hamiltonian Cycles and Paths
 - Traveling Salesman

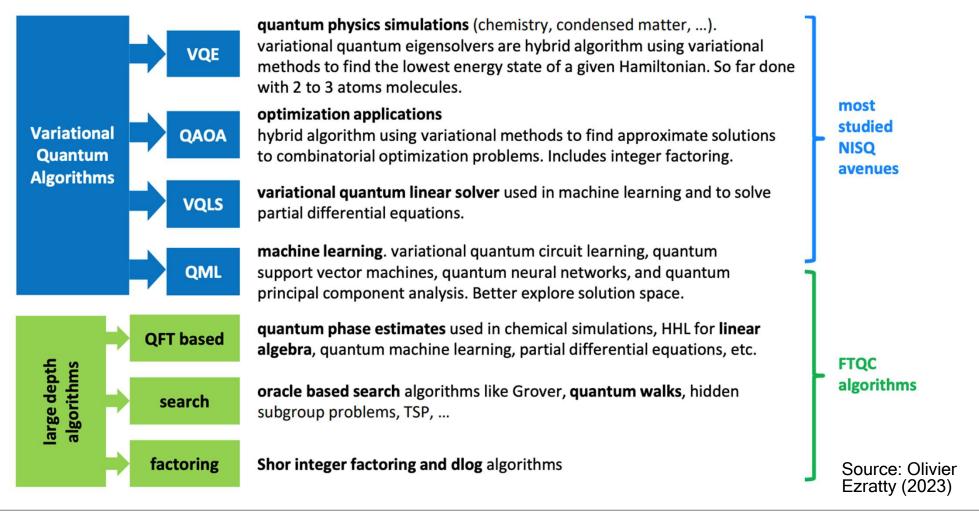
7. Tree Problems

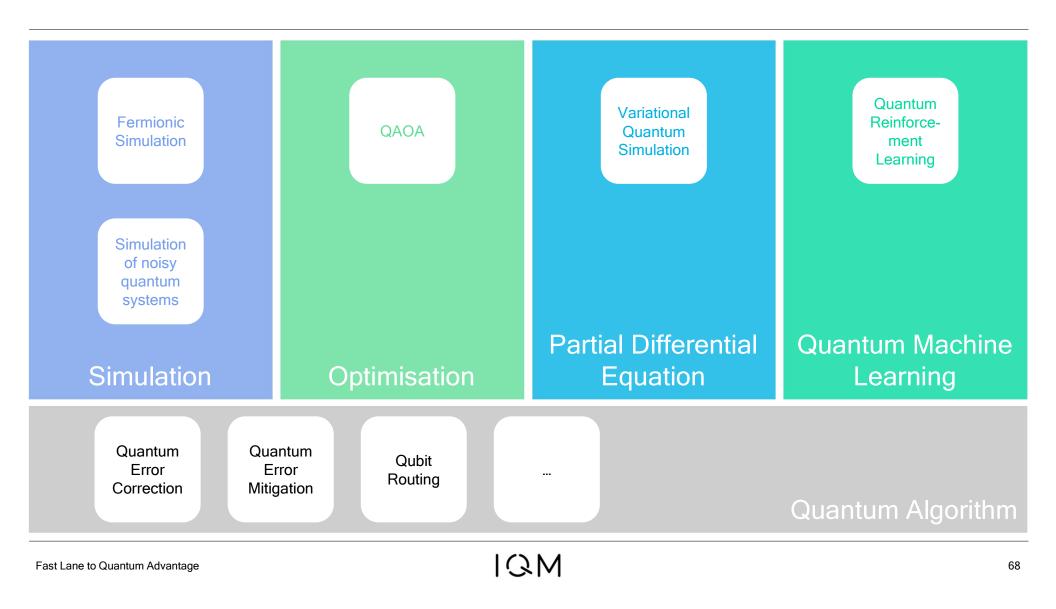
- Minimal Spanning Tree with a Maximal Degree Constraint
- Steiner Trees
- Directed Feedback Vertex Set
- Undirected Feedback Vertex Set
- Feedback Edge Set
- 8. Graph Isomorphisms



A. Lucas, *Ising formulations of many NP problems*, Frontiers in Physics 2, 5 (2014).

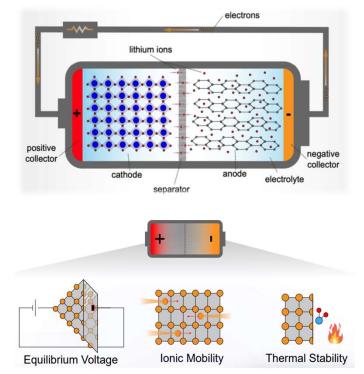
66





Real-world use-cases for different application areas

- Quantum Optimization: Power Plant Maintenance Scheduling with Energy Company Job-shop scheduling with resource constraints and specific time windows structure (QAOA variants)
- Quantum Simulation: Battery material design with Automotive Company Improve energy storage capabilities, charging and discharging speed and aging (Quantum Monte Carlo, DMFT)
- Quantum Machine Learning: Discovering Fraud with Insurance Company Anomaly detection in financial transactions to detect fraud such as money laundering

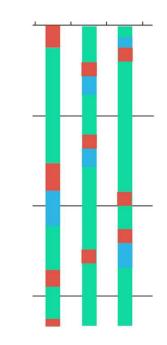


Real-world use-cases for different application areas

- Quantum Optimization: Power Plant Maintenance Scheduling with Energy Company Job-shop scheduling with resource constraints and specific time windows structure (QAOA variants)
- Quantum Simulation: Battery material design with Automotive Company

Improve energy storage capabilities, charging and discharging speed and aging (Quantum Monte Carlo, DMFT)

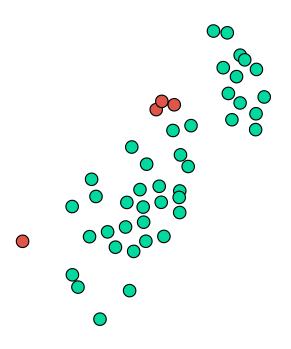
 Quantum Machine Learning: Discovering Fraud with Insurance Company Anomaly detection in financial transactions to detect fraud such as money laundering



Real-world use-cases for different application areas

- Quantum Optimization: Power Plant Maintenance Scheduling with Energy Company Job-shop scheduling with resource constraints and specific time windows structure (QAOA variants)
- Quantum Simulation: Battery material design with Automotive Company
 Improve energy storage capabilities, charging and discharging speed and aging (Quantum Monte Carlo, DMFT)
- Quantum Machine Learning: Discovering Fraud with Insurance Company

Anomaly detection in financial transactions to detect fraud such as money laundering



• Cost function
$$F(z_1, z_2, ..., z_n) = q \sum_{i,j=1}^n z_i z_j \sigma_{ij} - (1-q) \sum_{i=1}^n z_i \mu_i, \quad z_i = 0, 1$$

Portfolio weights $z_i = 0$ or 1 of stock *i*, expected return μ_i , the covariance matrix

of the stock returns σ_{ij} . q sets the risk preference of the investor: q = 1 if the investor wants to choose the portfolio with the lowest risk, irrespective of the return. q = 0 in the case of an aggressive investor who takes only the return of the stocks into account.

• Constraint for "feasible" portfolio, $\sum z_i = B$. The investment resource is limited.

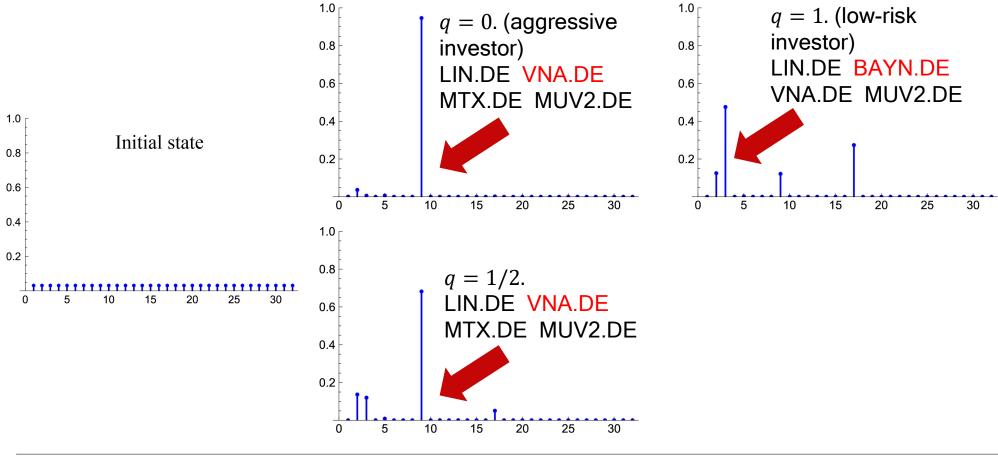
$$F^{(A)}(z_1, \dots, z_n) = F(z_1, \dots, z_n) + A \left(\sum_{i=1}^n z_i - B\right)^2.$$
 The last term is the penalty to pay if $\sum_{i=1}^n z_i = B$ is not observed.

• Take q = 0,1/2, and 1, n = 5, B = 4, A = 10 in the following.

From S. Brandhofer *et al.*, Benchmarking the performance of portfolio optimization with QAOA, Quantum Inf. Process. 22, 25 (2023).

Table 2 Return vector μ_i for 5 assets chosen from the German DAX 30

LIN.DE	BAYN.DE	E VN	A.DE	MTX.DE	MUV2.DE
0.26801758	-0.11724	968 0.2	109537	0.21523688	0.1128935
Table 3 Covar	riance matrix σ_{ij} for	or 5 assets chosen fr	rom the German D	AX 30	
	LIN.DE	BAYN.DE	VNA.DE	MTX.DE	MUV2.DE
LIN.DE	0.21117209	0.03030933	0.00941277	0.02972179	0.02922818
BAYN.DE	0.03030933	0.08796365	0.01833403	0.0465302	0.04069187
VNA.DE	0.00941277	0.01833403	0.04971719	0.02303918	0.02051608
MTX.DE	0.02972179	0.0465302	0.02303918	0.13717214	0.05638483
	0.02922818	0.04069187	0.02051608	0.05638483	0.06765634



Fast Lane to Quantum Advantage

IQM

q value	Stocks portfolio	cost	
q = 0 (aggressive investor)	LIN.DE VNA.DE MTX.DE MUV2.DE	-0.00238912	
q = 1/2	LIN.DE VNA.DE MTX.DE MUV2.DE	-0.807102	
q = 1 (low-risk investor)	LIN.DE BAYN.DE VNA.DE MUV2.DE	0.713494	

Conclusion: Quantum algorithms

- NISQ devices can run specific algorithms that might offer an edge over classical algorithms, even in the presence of noise.
- The prevalent paradigm for NISQ quantum algorithms, such as QAOA, is to prepare them for execution in a hybrid manner, utilizing both quantum and classical computing resources
- Quantum algorithms like QAOA are adaptable to a range of problems. Developing a deeper understanding of suitable problems and how they are mapped is essential
- Achieving early quantum advantage requires the strategic alignment of purpose-built algorithms with targeted problems and the compatible hardware

IQM Academy

Gain a thorough understanding of quantum computing and its applications.

- A free curriculum and learning platform for anyone
- Easy to pick up, no previous knowledge required
- Highly interactive and engaging

Start today on

https://academy.meetiqm.com/

