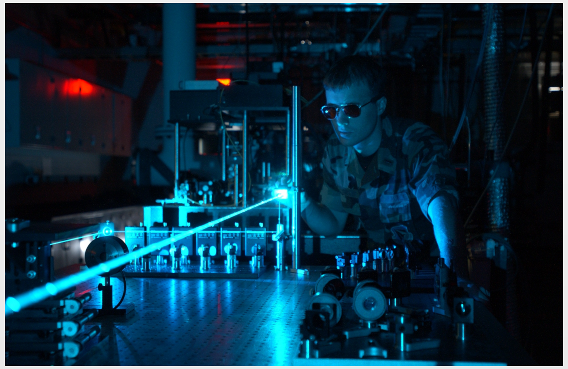
Quantum Technologies: what, how and for whom?

Iordanis Kerenidis

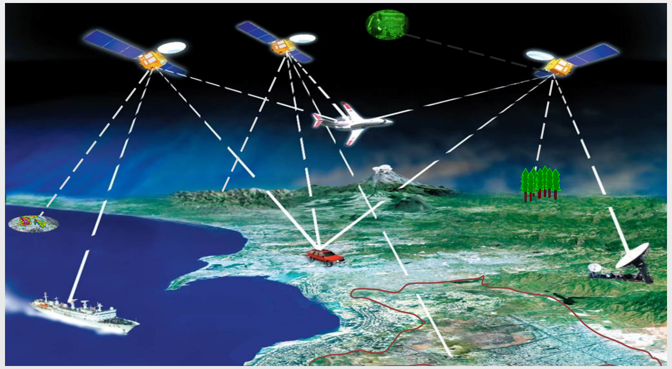
Paris Centre for Quantum Computing PCQC, CNRS Paris
QC WARE, Palo Alto USA & Paris France

Quantum Mechanics

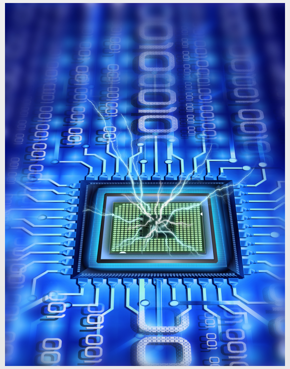
The first quantum revolution



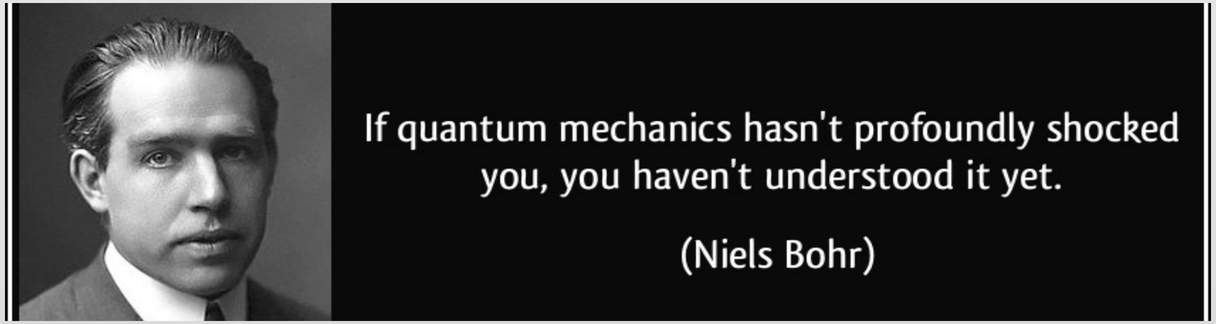
laser



GPS

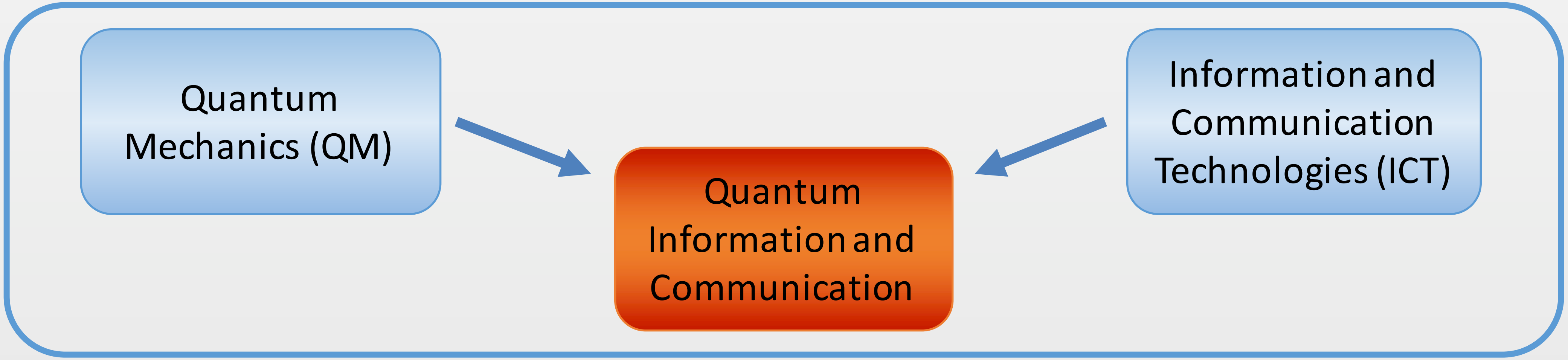


microelectronics



Basic Science

Quantum Information Communication Technologies

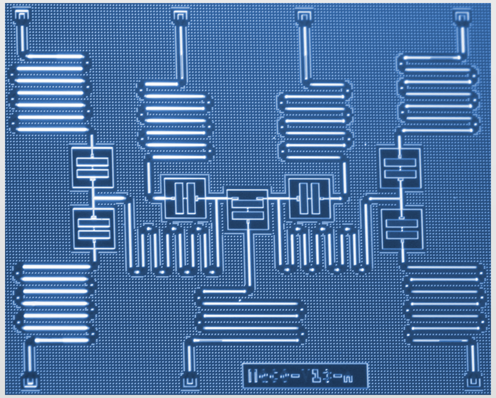


Quantum Information Communication Technologies

Quantum Mechanics (QM)

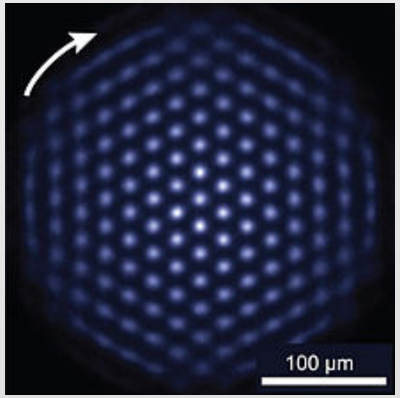
Quantum Information and Communication

Information and Communication Technologies (ICT)



Computers

Communications and cryptography



Simulators

The beginning: Quantum simulation

Problem

Simulate the behaviour of quantum systems
(track exponential number of parameters)

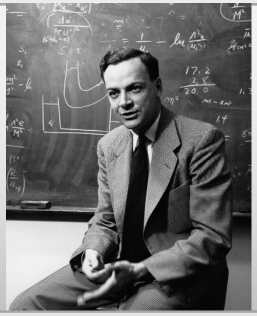
The beginning: Quantum simulation

Problem

Simulate the behaviour of quantum systems
(track exponential number of parameters)

Feynman's Idea ['80s]

Use quantum systems to simulate quantum systems.



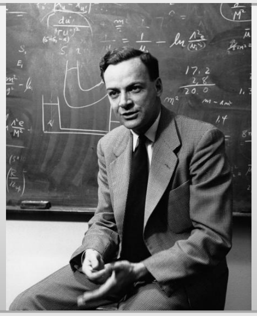
The beginning: Quantum simulation

Problem

Simulate the behaviour of quantum systems
(track exponential number of parameters)

Feynman’s Idea ['80s]

Use quantum systems to simulate quantum systems.



Applications of quantum simulation

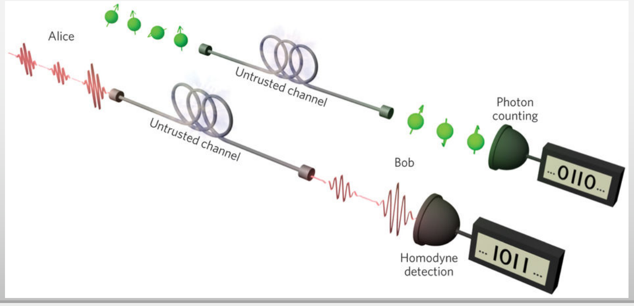
Quantum chemistry: simulation of small molecules

Drug development

Quantum cryptography & communications

Quantum Key distribution

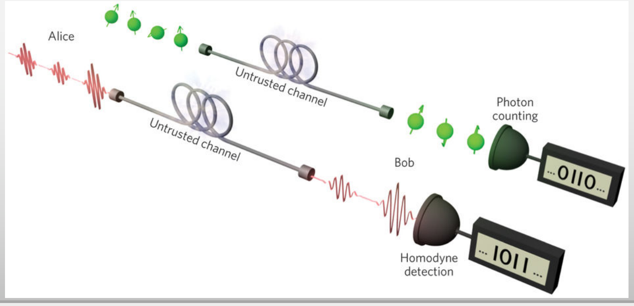
Unconditional security
Commercialization
Worse key rates, more expensive



Quantum cryptography & communications

Quantum Key distribution

Unconditional security
Commercialization
Worse key rates, more expensive



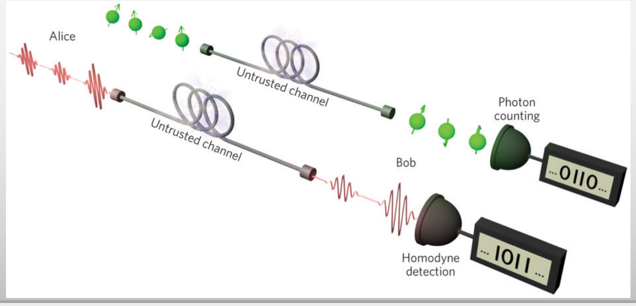
Quantum properties

No cloning: the adversary cannot copy the messages
Observation disturbance: observing quantum systems disturbs them

Quantum cryptography & communications

Quantum Key distribution

Unconditional security
Commercialization
Worse key rates, more expensive



Quantum properties

No cloning: the adversary cannot copy the messages
Observation disturbance: observing quantum systems disturbs them

Factoring

Breaking RSA
NIST Competition

287,365,167,584,786,166,284,179,185,016,920,089,269,094,158,453,856,165,125,
203,406,541,318,870,452,164,142,161,028,497,034,055,908,330,795,850,575,194,
401,741,649,307,604,240,081,597,502,233,885,902,517,289,285,023,585,791,712,
232,223,239,592,783,051,318,295,484,219,924,025,332,854,246,132,728,715,500,
942,552,460,619,944,194,679,330,033,676,282,829,328,152,739,714,673,366,108,
373,179,906,823,029,877,973,507,929,239,423,443,377,132,384,753,724,178,388,
993,447,226,041,912,767,138,249,925,309,993,357,379,153,572,212,166,426,529,
200,773,538,079,561,418,021,293,020,569,682,116,684,933,148,131,688,925,170,
517,608,523,929,010,548,063,794,858,755,212,639,973,154,477,995,891,903,128,
142,914,896,767,233,157,948,181,644,383,905,584,704,750,296,848,115,761,338,
451,704,955,875,653,862,778,035,566,296,235,473,942,689,241,421,722,455,033,
259,091,237,726,940,399,605,388,375,173,453,263,419,405,930,790,375,958,488,
745,081,259,142,857,304,624,751,178,998,559,654,155,353,368,257,669,344,697,
052,122,166,097,011,178,766,722,819,809,221,811,483,063,408,587,293,703,035,
253,584,044,846,944,373,009,650,823,628,883,576,287,986,355,136,594,363,446,
417,487,937,702,394,428,523,166,278,061,088,262,825,840,876,874,574,984,169,

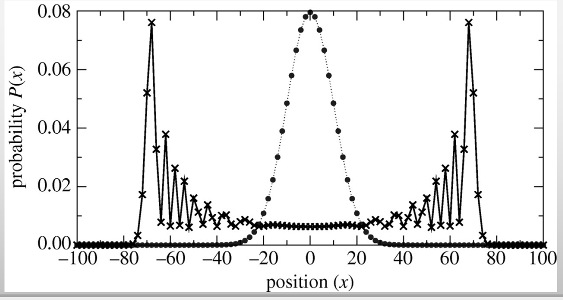
Quantum Computing

Use cases, challenges and potential

Quantum Computing

Quantum walks, Search, query algorithms

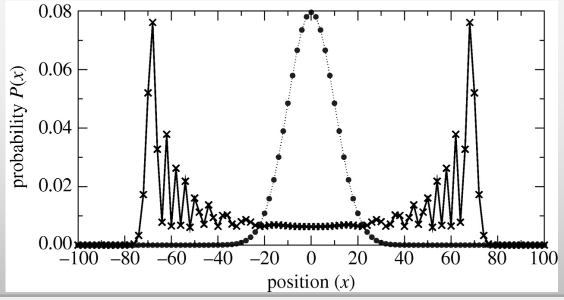
Mostly quadratic speed ups



Quantum Computing

Quantum walks, Search, query algorithms

Mostly quadratic speed ups



The HHL algorithm [Harrow, Hassidim, Lloyd 2009]

Quantum computers provide a quantum solution to a system of linear equations in certain cases exponentially faster than classical algorithms.

"It opens the possibility of dramatic speedups for machine learning tasks, richer models for data sets and more natural settings for learning and inference"

Quantum Machine Learning Workshop during NIPS 2015

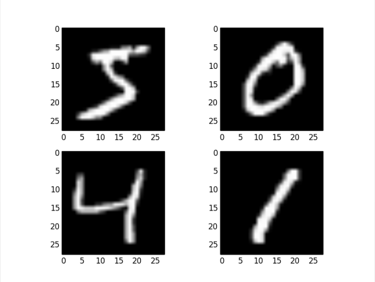
Quantum Machine Learning

Use cases, challenges and potential

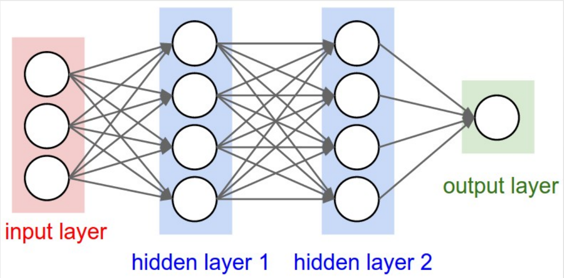
Machine Learning Applications

Quantum recommendation systems
[Kerenidis, Prakash ’17]

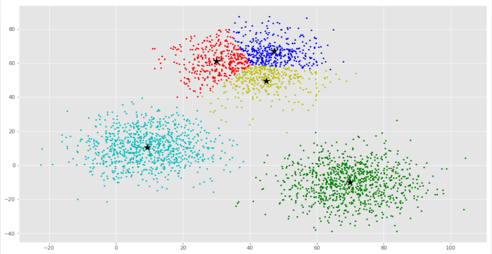
Quantum algorithms for image recognition
[Kerenidis, Luongo ’18]



Quantum neural networks
[Allcock, Hsieh, Kerenidis, Zhang 18]



Quantum algorithms for clustering
[Kerenidis, Landman, Luongo, Prakash 18]



Recommendation Systems [Kerenidis, Prakash, arXiv:1603.08675]

amazon

Step 1

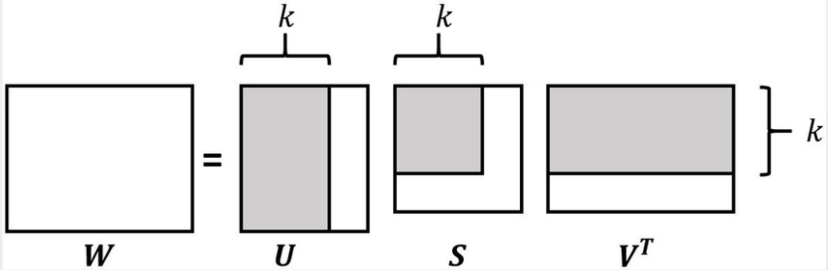
Products

Users

?	**1**	**…**	**?**
?	0	…	?
…	…	…	…
1	?	…	0

Step 2

Singular Value Estimation



Step 3

Efficient quantum algorithm for Singular Value Estimation

Quantum computers provide competitive recommendations fast!

Classification of MNIST dataset [Kerenidis,Luongo, arXiv:1805.08837]

Accuracy: 98.5%

Running time (n images, d-dimensions)

Classical: $O(n\ d^2) \sim 10^{13}$ (1 hour on 6Tb RAM HPC)
Quantum: $O(\kappa, \mu, 1/\theta, 1/\delta, 1/\eta, K, \log(n, d, 1/\varepsilon)) \sim 10^7$

Hope (and some evidence)

Quantum classification algorithms can handle bigger dimensions (hence in many cases be more accurate), since their running time scales more favorably with the dimension.

Q Neural Nets [Allcock, Hsieh, Kerenidis, Zhang, arXiv:1812.03089]

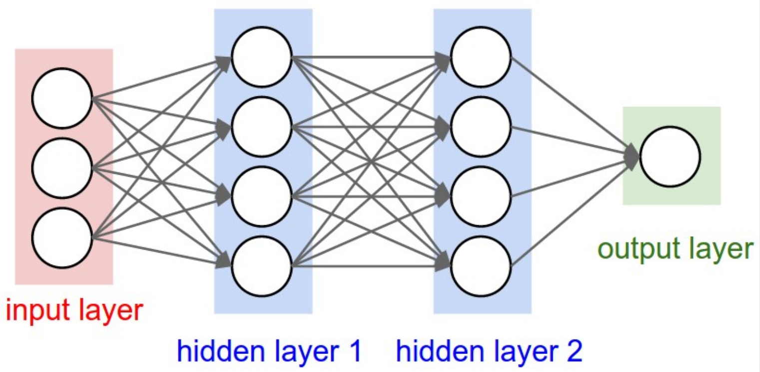
Feedforward/backpropagation algorithms

- Distance estimation in superposition
- Quantum Linear algebra
- Clever weight storage

Accuracy: similar to classical feedforward NNs

Running time: scales as O(Neurons)

[classical as O(Edges)] $\tilde{O}\left((TM)^{1.5} N \frac{\log(1/\gamma)}{\epsilon} R\right)$



q-means clustering [Kerenidis,Landman,Luongo,Prakash, arXiv:1812.03584]

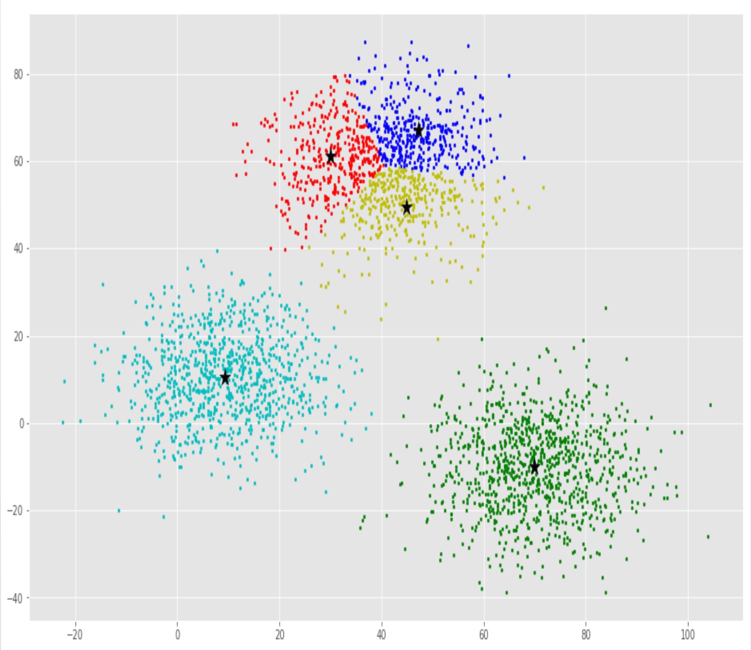
K-means

Input: N points in d-dimensions

1. Start with some random points as centroids

Repeat until convergence

2. For each point
   estimate distances to centroids and assign to closest cluster
3. Update the centroids



q-means clustering [Kerenidis,Landman,Luongo,Prakash, arXiv:1812.03584]

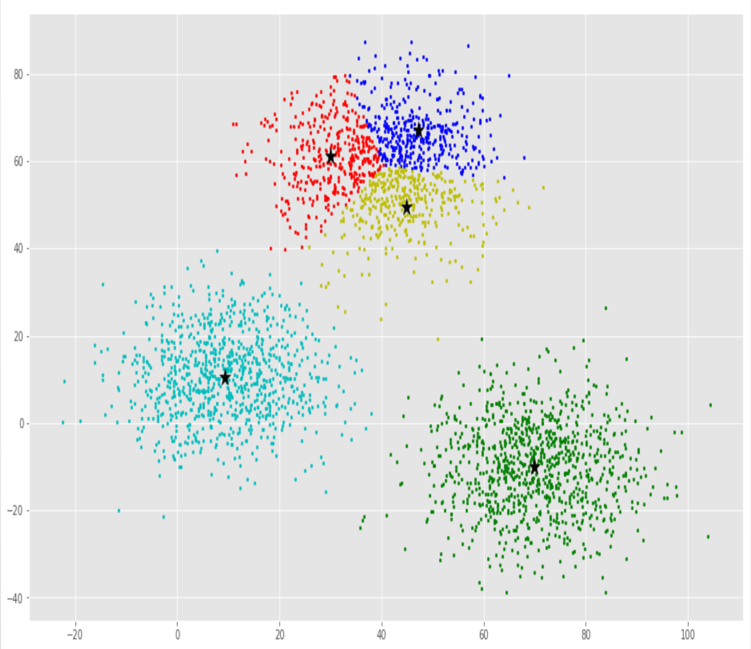
q-means

Input: N points in d-dimensions (quantum access)

1. Start with some random points as centroids

Repeat until convergence

2. For all points in superposition
   estimate distances to centroids and assign to closest cluster
3. Update the centroids
   i. Quantum linear algebra to find new centroid
   ii. Tomography to recover classical description

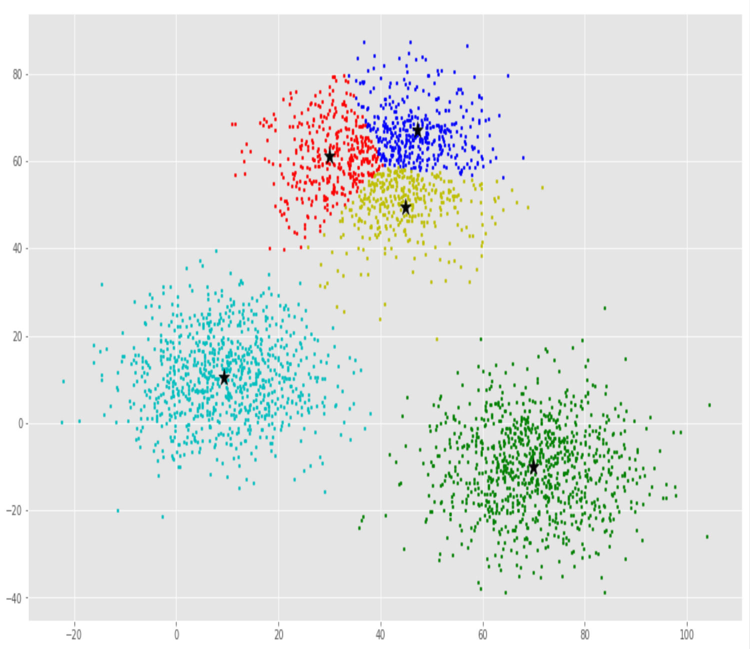


q-means clustering [Kerenidis,Landman,Luongo,Prakash, arXiv:1812.03584]

Accuracy: similar to robust classical k-means

Running time: [N d-dimensional points, K clusters]

Classical: O(K d N)
Quantum: O(K d logN)



Bringing QML towards the NISQ era

1. Will QC ever be useful for Machine learning?
   a. We are designing and rigorously analyzing new QML algorithms (Exp. Max, Reinforcement Learning, Convolution NNs, …)
   b. We optimize the most promising ones for specific use cases

Bringing QML towards the NISQ era

1. Will QC ever be useful for Machine learning?
   a. We are designing and rigorously analyzing new QML algorithms (Exp. Max, Reinforcement Learning, Convolution NNs, …)
   b. We optimize the most promising ones for specific use cases

2. How soon will QC be useful? (Resource analysis)
   a. We are building QML APIs based on linear algebra subroutines, in order to benchmark the practical behavior of quantum machine learning algorithms on real data, using both simulators and real hardware.

Bringing QML towards the NISQ era

1. Will QC ever be useful for Machine learning?
   a. We are designing and rigorously analyzing new QML algorithms (Exp. Max, Reinforcement Learning, Convolution NNs, …)
   b. We optimize the most promising ones for specific use cases

2. How soon will QC be useful? (Resource analysis)
   a. We are building QML APIs based on linear algebra subroutines, in order to benchmark the practical behavior of quantum machine learning algorithms on real data, using both simulators and real hardware.

3. Can we push some ML use cases to the NISQ era?
   a. We are designing new heuristics/algorithms for specific hardware
   b. We implement meaningful scaled-down versions on various hardware
   c. We benchmark hardware platforms through ML applications

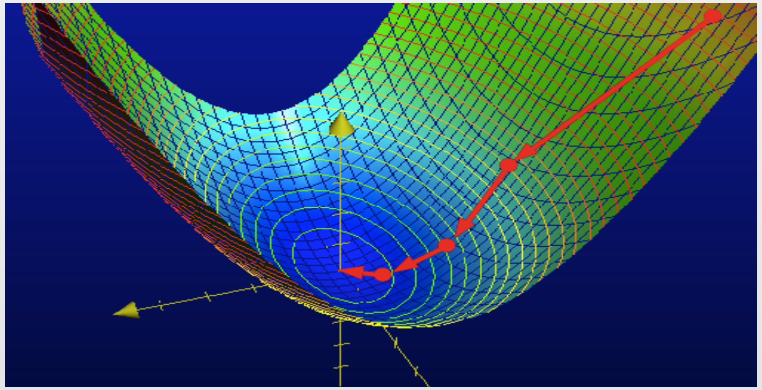
Quantum Optimization

Use cases, challenges and potential

Iterative methods [Kerenidis, Prakash arXiv:1704.04992, arXiv:1808.09266]

General Method

1. Start with an initial solution.
2. Update the solution according to Update Rule
3. Repeat until the solution is satisfactory



Gradient Descent

Quantum algorithms for affine gradients using Linear System Solvers (can run in cases exponentially faster)

Interior Point Methods

Quantum algorithms for convex optimization with polynomial time savings.

Iterative methods [Kerenidis, Prakash arXiv:1704.04992, arXiv:1808.09266]

General Method

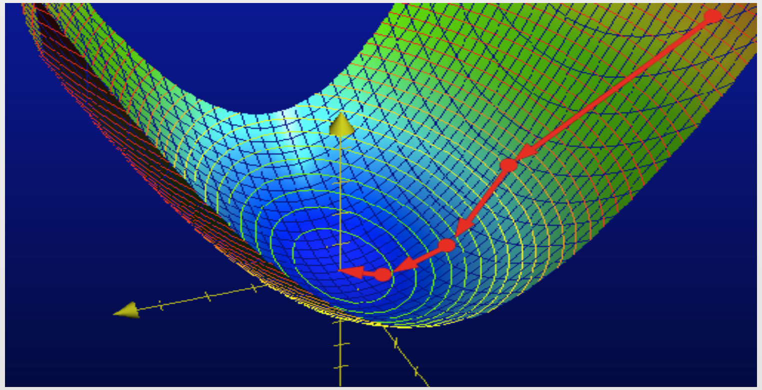
1. Start with an initial solution.
2. Update the solution according to Update Rule
3. Repeat until the solution is satisfactory

Gradient Descent

Linear Regression, Weighted Least Squares,
Neural Net training

Interior Point Methods

Portfolio Optimization, Support Vector Machines,
Quadratic and Second Order Cone Programming



Combinatorial Optimization

NP-complete problems

1. Traveling Salesman
2. Integer Programming
3. MAX-SAT, MAX-CUT

Quantum Algorithms

Quadratic improvement (Grover's search)

Quantum Heuristics

Quantum Approximate Optimization Algorithm
Variational Quantum Eigensolvers

Conclusions

1. Quantum technologies have the potential to revolutionize information and communication technologies
2. It will be a long but highly exciting journey
3. The time is right to investigate how quantum computing can disrupt your industry