Introduction to Quantum Computing

Lecture 3

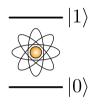
Stefan Kühn
DESY Summer Student Program, 18.08.2025



Recap of the previous lecture

Qubits

- > Quantum mechanical two-level systems $\mathcal{H} = \{\ket{0}, \ket{1}\}$
- > Can be in superposition
- Mulitple qubits can be entangled



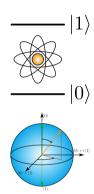
Recap of the previous lecture

Qubits

- > Quantum mechanical two-level systems $\mathcal{H} = \{|0\rangle, |1\rangle\}$
- > Can be in superposition
- > Mulitple qubits can be entangled

Quantum gates

- > Quantum gates: unitary operations on a single/few qubits
- Combining quantum gates we can express any unitary operation



Recap of the previous lecture

Qubits

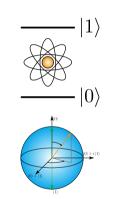
- > Quantum mechanical two-level systems $\mathcal{H} = \{|0\rangle, |1\rangle\}$
- > Can be in superposition
- Mulitple qubits can be entangled

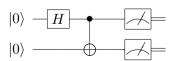
Quantum gates

- > Quantum gates: unitary operations on a single/few qubits
- Combining quantum gates we can express any unitary operation

Quantum circuits

- Combining quantum gates we can express any unitary operation
- Measurement reveals information about the system





Outline

The Deutsch-Josza algorithm

Grover's algorithm

Complexity theory

Hybrid quantum-classical algorithms

Challenges for hybrid quantum-classical algorithms

1.

The Deutsch-Josza algorithm

Grover's algorithm

Complexity theory

Hybrid quantum-classical algorithms

Challenges for hybrid quantum-classical algorithms

Setting

- ightharpoonup Given: a function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ that is promised to be constant or balanced
- > Task: find out if f is constant or balanced

Setting

- **>** Given: a function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ that is promised to be constant or balanced
- > Task: find out if f is constant or balanced
- Classical computer: try more than half of the possible inputs

$$\Rightarrow \frac{1}{2} \times 2^n + 1 = 2^{n-1} + 1$$
 function calls

x_0	x_1	$f(x_0, x_1)$
0	0	1
0	1	1
1	0	0
1	1	0

Setting

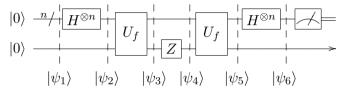
- **>** Given: a function $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$ that is promised to be constant or balanced
- > Task: find out if f is constant or balanced
- Classical computer: try more than half of the possible inputs

$$\Rightarrow \frac{1}{2} \times 2^n + 1 = 2^{n-1} + 1$$
 function calls

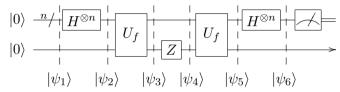
> Let us assume we have a unitary $U_f \ket{x}\ket{y} = \ket{x}\ket{y \oplus f(x)}$

$$|x\rangle$$
 $\xrightarrow{n/}$ U_f $|y \oplus f(x)\rangle$

 $> U_f$ is called an **oracle**



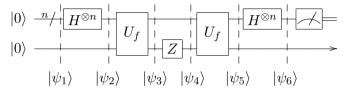
$$|\psi_1\rangle = |0...0\rangle |0\rangle$$



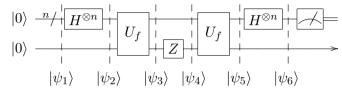
$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

1
$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

2 $|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$



- $|\psi_1\rangle = |0...0\rangle |0\rangle$
- $|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$
- $|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$



$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_{x}^{\infty} (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_x (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_x (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_5\rangle = \sum_x (-1)^{f(x)} |x\rangle |f(x) \oplus f(x)\rangle = \sum_x (-1)^{f(x)} |x\rangle |0\rangle$$

$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_5\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |f(x) \oplus f(x)\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |0\rangle$$

$$f(x)$$
 constant

$$f(x)$$
 balanced

$$|\psi_5\rangle = \pm \sum_x |x\rangle |0\rangle$$

Deutsch-Josza algorithm

$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

3
$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_x (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_5\rangle = \sum_{x}^{x} (-1)^{f(x)} |x\rangle |f(x) \oplus f(x)\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |0\rangle$$

$$f(x)$$
 constant

f(x) balanced

$$|\psi_5\rangle = \pm \sum_x |x\rangle |0\rangle$$

$$|\psi_6\rangle = \pm |0...0\rangle |0\rangle$$

$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_5\rangle = \sum_{x}^{x} (-1)^{f(x)} |x\rangle |f(x) \oplus f(x)\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |0\rangle$$

$$f(x)$$
 constant

$$f(x)$$
 balanced

$$|\psi_5\rangle = \pm \sum_x |x\rangle |0\rangle$$

$$|\psi_6\rangle = \pm |0...0\rangle |0\rangle$$

Deutsch-Josza algorithm

$$|\psi_1\rangle = |0...0\rangle |0\rangle$$

$$|\psi_2\rangle = (|0\rangle + |1\rangle)^{\otimes n} |0\rangle = (\sum_x |x\rangle) |0\rangle$$

$$|\psi_3\rangle = \sum_x |x\rangle |0 \oplus f(x)\rangle = \sum_x |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |f(x)\rangle$$

$$|\psi_5\rangle = \sum_{x}^{x} (-1)^{f(x)} |x\rangle |f(x) \oplus f(x)\rangle = \sum_{x} (-1)^{f(x)} |x\rangle |0\rangle$$

$$f(x)$$
 constant

f(x) balanced

$$|\psi_5\rangle = \pm \sum_x |x\rangle |0\rangle$$

$$|\psi_5\rangle \perp |\phi\rangle = \sum_y |y\rangle |0\rangle$$

$$|\psi_6\rangle = \pm |0...0\rangle |0\rangle$$

$$0 = \langle \phi | \psi_5 \rangle = \langle \phi | H^{\otimes n} H^{\otimes n} | \psi_5 \rangle = (\langle 0...0 | \langle 0 |) | \psi_6 \rangle$$

- Quantum algorithm allows for deciding whether f is balanced or not with two calls to the oracle (independent of n)
- > Query the oracle in superposition
- Constructive interference (destructive interference) yields an unity (zero) amplitude in the constant (balanced) case

Deutsch-Josza algorithm

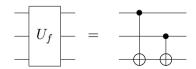
- Quantum algorithm allows for deciding whether f is balanced or not with two calls to the oracle (independent of n)
- > Query the oracle in superposition
- Constructive interference (destructive interference) yields an unity (zero) amplitude in the constant (balanced) case

The Deutsch-Josza algorithm needs exponentially fewer calls to the oracle than the classical algorithm.

Deutsch-Josza algorithm on quantum hardware

> Example for n=2 input bits and the following Boolean function

x_0	x_1	$f(x_0, x_1)$
0	0	0
0	1	1
1	0	1
1	1	0

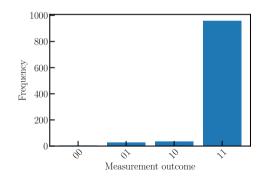


Deutsch-Josza algorithm on quantum hardware

> Example for n=2 input bits and the following Boolean function

	x_0	x_1	$f(x_0, x_1)$
	0	0	0
	0	1	1
	1	0	1
	1	1	0
_		_	—
	U_f	_ =	

 Results on actual quantum hardware (ibmq_lagos)



2.

The Deutsch-Josza algorithm

Grover's algorithm

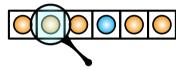
Complexity theory

Hybrid quantum-classical algorithms

Challenges for hybrid quantum-classical algorithms

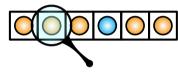
Description of the problem

> Goal: find an element in an unstructured database



Description of the problem

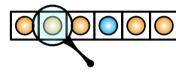
> Goal: find an element in an unstructured database



- > Given:
 - A set of N elements $\{x_0, x_1, \dots, x_{N-1}\}$
 - A function $f: \{x_0, x_1, \dots, x_{N-1}\} \to \mathbb{Z}_2$
 - An element x_k is called iff **marked** $f(x_k) = 1$
- > Task:
 - Find the marked element(s) in the data base

Description of the problem

> Goal: find an element in an unstructured database



- > Given:
 - A set of N elements $\{x_0, x_1, \dots, x_{N-1}\}$
 - A function $f: \{x_0, x_1, \dots, x_{N-1}\} \to \mathbb{Z}_2$
 - An element x_k is called iff **marked** $f(x_k) = 1$
- > Task:
 - Find the marked element(s) in the data base
- > Best classical solution: go through the elements one by one or try elements randomly
 - \Rightarrow Access the database $\mathcal{O}(N)$ times

Comments

- > If the database is sorted, the element can be found in $\mathcal{O}(\log N)$ time, however sorting the database takes $\mathcal{O}(N\log N)$
 - ⇒ Depending on the problem sorting might not pay off
- The problem essentially corresponds to function inversion: find the element that produces a certain output of the function
 - ⇒ Brute-force attack in symmetric cryptography
- > Many problems can be cast into such a form, e.g. satisfiablity of a Boolean clause

Basic overview

- > Quantum algorithm that allows for solving the problem described before with $\mathcal{O}(\sqrt{N})$ to an oracle implementing f
 - \Rightarrow Polynomial speedup

Basic overview

- > Quantum algorithm that allows for solving the problem described before with $\mathcal{O}(\sqrt{N})$ to an oracle implementing f
 - ⇒ Polynomial speedup
- The different elements of the database are encoded in the different basis states

$$x_0 \equiv |x_0\rangle = |000\rangle$$
 $x_2 \equiv |x_2\rangle = |010\rangle$ $x_4 \equiv |x_4\rangle = |100\rangle$ $x_6 \equiv |x_6\rangle = |110\rangle$
 $x_1 \equiv |x_1\rangle = |001\rangle$ $x_3 \equiv |x_3\rangle = |011\rangle$ $x_5 \equiv |x_5\rangle = |101\rangle$ $x_7 \equiv |x_7\rangle = |111\rangle$

Basic overview

- > Quantum algorithm that allows for solving the problem described before with $\mathcal{O}(\sqrt{N})$ to an oracle implementing f
 - ⇒ Polynomial speedup
- The different elements of the database are encoded in the different basis states

$$x_0 \equiv |x_0\rangle = |000\rangle \qquad x_2 \equiv |x_2\rangle = |010\rangle \qquad x_4 \equiv |x_4\rangle = |100\rangle \qquad x_6 \equiv |x_6\rangle = |110\rangle$$
$$x_1 \equiv |x_1\rangle = |001\rangle \qquad x_3 \equiv |x_3\rangle = |011\rangle \qquad x_5 \equiv |x_5\rangle = |101\rangle \qquad x_7 \equiv |x_7\rangle = |111\rangle$$

- Starting from an equal-weight superposition of all basis states, one uses amplitude amplification to single out the marked element
 - Oracle
 - Diffusion operator

L.K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing 212 - 219 (1996)

Basic overview

- > Quantum algorithm that allows for solving the problem described before with $\mathcal{O}(\sqrt{N})$ to an oracle implementing f
 - ⇒ Polynomial speedup
- The different elements of the database are encoded in the different basis states

$$x_0 \equiv |x_0\rangle = |000\rangle \qquad x_2 \equiv |x_2\rangle = |010\rangle \qquad x_4 \equiv |x_4\rangle = |100\rangle \qquad x_6 \equiv |x_6\rangle = |110\rangle$$
$$x_1 \equiv |x_1\rangle = |001\rangle \qquad x_3 \equiv |x_3\rangle = |011\rangle \qquad x_5 \equiv |x_5\rangle = |101\rangle \qquad x_7 \equiv |x_7\rangle = |111\rangle$$

- > Starting from an equal-weight superposition of all basis states, one uses **amplitude amplification** to single out the marked element
 - Oracle
 - Diffusion operator
- > Measure the final state to lobiain raceandidate for the marked relement for computing 212 219 (1996)

The oracle

- > We need to implement the function f on a quantum computer
- > This is done in form of an oracle

$$U_f |x_i\rangle = (-1)^{f(x_i)} |x_i\rangle, \qquad U_f = \mathbb{1} - 2 |m\rangle\langle m|$$

The oracle

- > We need to implement the function f on a quantum computer
- > This is done in form of an **oracle**

$$U_f |x_i\rangle = (-1)^{f(x_i)} |x_i\rangle, \qquad U_f = \mathbb{1} - 2 |m\rangle\langle m|$$

> Effect of the oracle on a wave function $|\psi
angle = \sum_i c_i \, |x_i
angle$



> While U_f has an effect on $|\psi\rangle$ this effect cannot be measured, as a measurement only reveals information about $|c_i|^2$

L. K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing 212 – 219 (1996)

The oracle

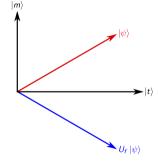
> To understand the effect of U_f further it is advantageous to separate the wave function $|\psi\rangle$ in a component parallel to $|m\rangle$ and one orthogonal to it

$$|\psi\rangle = c_i |m\rangle + \underbrace{\sum_{i \neq m} c_i |x_i\rangle}_{|t\rangle}$$

The oracle

> To understand the effect of U_f further it is advantageous to separate the wave function $|\psi\rangle$ in a component parallel to $|m\rangle$ and one orthogonal to it

$$|\psi\rangle = c_i |m\rangle + \underbrace{\sum_{i \neq m} c_i |x_i\rangle}_{|t\rangle}$$



> U_f reflects $|\psi\rangle$ around $|t\rangle$

L. K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing 212 – 219 (1996)

The diffusion operator

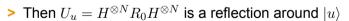
- > Let $|u\rangle = H^{\otimes N} |0\dots 0\rangle$ \Rightarrow Uniform superposition of all 2^N basis states
- > Let R_0 be the reflection around $|0...0\rangle$

$$R_0 \left| y
ight
angle = egin{cases} + \left| y
ight
angle & ext{iff } \left| y
ight
angle = \left| 0...0
ight
angle \ - \left| y
ight
angle \, , & ext{otherwise}. \end{cases}$$

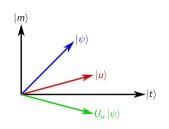
The diffusion operator

- \rightarrow Let $|u\rangle = H^{\otimes N} |0\dots 0\rangle$
- \Rightarrow Uniform superposition of all 2^N basis states
- > Let R_0 be the reflection around $|0\dots 0\rangle$

$$R_0 \left| y
ight
angle = egin{cases} + \left| y
ight
angle & ext{iff } \left| y
ight
angle = \left| 0...0
ight
angle \ - \left| y
ight
angle , & ext{otherwise}. \end{cases}$$



- $> U_u$ is called **Grover's diffusion operator**
- It corresponds to a reflection of the amplitudes around the mean value $\mu=rac{1}{N}\sum_i c_i$ L.K. Grover, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing 212 – 219 (1996)

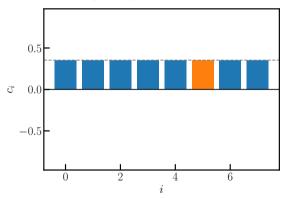


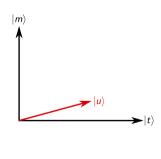
The Grover iteration

- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function

The Grover iteration

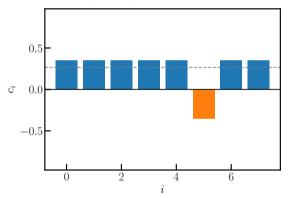
- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function

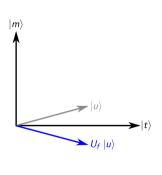




The Grover iteration

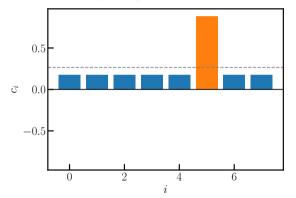
- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function

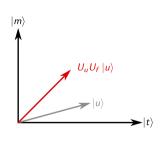




The Grover iteration

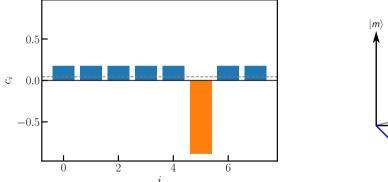
- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function

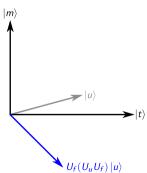




The Grover iteration

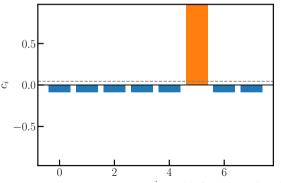
- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function

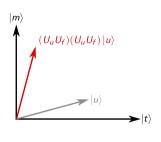




The Grover iteration

- > Start from the equal-weight superposition state $|\psi\rangle = |u\rangle = H^{\otimes N} |0\dots 0\rangle$
- > Repeatedly apply the oracle and the diffusion operator U_uU_f to the wave function





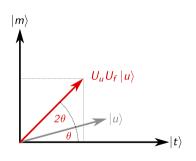
The Grover iteration

> After *k* iterations the wave function is of the form

$$\begin{aligned} |\psi_k\rangle &= (U_uU_f)^k \, |\psi\rangle = (U_uU_f)^k \, |u\rangle \\ &= \sin\bigl((2k+1)\theta\bigr) \, |m\rangle + \cos\bigl((2k+1)\theta\bigr) |t\rangle \end{aligned}$$

> If $\cos((2k+1)\theta)$ vanishes we are left with $|m\rangle$

$$(2k+1)\theta = \frac{\pi}{2} \quad \Leftrightarrow \quad \theta = \frac{\pi}{2(2k+1)} \approx \frac{\pi}{4k}$$



Complexity of the algorithm

 \triangleright How does the optimal k depend on N?

Complexity of the algorithm

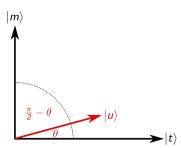
- > How does the optimal k depend on N?
- This can be determined with a simple geometrical picture

$$\begin{split} \sin(\theta) &= \cos\left(\frac{\pi}{2} - \theta\right) \\ &= \left\langle m|u\right\rangle = \left\langle m\big|H^{\otimes n}\big|00\dots 0\right\rangle = \frac{1}{\sqrt{N}} \end{split}$$

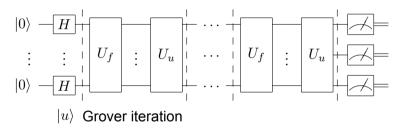
> For large values of N we can approximate

$$\theta \approx 1/\sqrt{N} \approx \pi/4k$$

Overall complexity $\mathcal{O}(\sqrt{N})$ Grover. Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing 212 – 219 (1996)



Quantum circuit for Grover's algorithm



- lacksquare Initial layer of Hadamard gates prepares the equal-weight superposition |u
 angle
- > Subsequent layers correspond do Grover iterations consisting of the oracle U_f and the diffusion operator U_u amplifying the amplitude of the marked element
- Final measurement reveals the probability distribution of basis states

Comments

> It is important to choose the right number of iterations, coefficient of $|m\rangle$ is given by

$$\sin((2k+1)\theta)$$

 \Rightarrow It oscillates periodically in k assuming a small value of θ

Comments

> It is important to choose the right number of iterations, coefficient of $|m\rangle$ is given by

$$\sin((2k+1)\theta)$$

- \Rightarrow It oscillates periodically in k assuming a small value of θ
- > $|\psi\rangle$ will have a dominant component $|m\rangle$ at the end, but there might be small other components
- A single measurement at the end might not reveal the element, but a few repetitions should be sufficient

Comments

> It is important to choose the right number of iterations, coefficient of $|m\rangle$ is given by

$$\sin((2k+1)\theta)$$

- \Rightarrow It oscillates periodically in k assuming a small value of θ
- > $|\psi\rangle$ will have a dominant component $|m\rangle$ at the end, but there might be small other components
- A single measurement at the end might not reveal the element, but a few repetitions should be sufficient
- igwedge We assume that we have f in form of the oracle U_f
 - \Rightarrow If we have to go through all the elements to construct U_f this is not helpful!
- If one has additional knowledge on how to implement f one can often do better using a classical algorithm

3.

The Deutsch-Josza algorithm

Grover's algorithm

Complexity theory

Hybrid quantum-classical algorithms

Challenges for hybrid quantum-classical algorithms

Solving problems on a quantum computer

- Many more known quantum algorithms that (might) perform better than the best known classical algorithms
 - Shor's factoring algorithm
 - Grover's search algorithm
 - HHL algorithm for linear equations

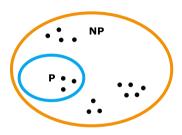
- Quantum Simulation
- Bernstein–Vazirani algorithm
- **.**
- Exploiting quantum features such as superposition and entanglement these algorithms can outperform the best known classical algorithms

Solving problems on a quantum computer

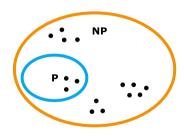
- Many more known quantum algorithms that (might) perform better than the best known classical algorithms
 - Shor's factoring algorithm
 - Grover's search algorithm
 - HHL algorithm for linear equations
- Quantum Simulation
- Bernstein-Vazirani algorithm

Exploiting quantum features such as superposition and entanglement these algorithms can outperform the best known classical algorithms

Which problems can be solved efficiently on quantum computers?

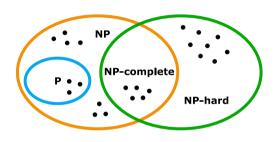


- P: decision problems solvable by a deterministic Turing machine in polynomial time
- NP: decision problems solvable by a non-deterministic Turing machine in polynomial time
 - Solution can be checked on a deterministic Turing machine in polynomial time

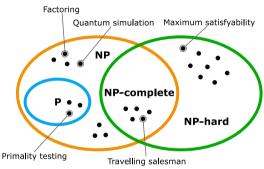


- P: decision problems solvable by a deterministic Turing machine in polynomial time
- NP: decision problems solvable by a non-deterministic Turing machine in polynomial time
 - Solution can be checked on a deterministic Turing machine in polynomial time

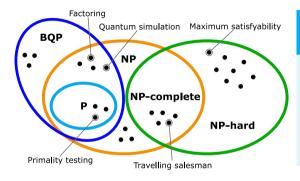
Since an exponential function grows asymptotically faster than any polynomial problems in P are considered the "easy" ones, and the problems in NP are considered the "hard" ones



- P: decision problems solvable by a deterministic Turing machine in polynomial time
- NP: decision problems solvable by a non-deterministic Turing machine in polynomial time
 - Solution can be checked on a deterministic Turing machine in polynomial time
- Since an exponential function grows asymptotically faster than any polynomial problems in P are considered the "easy" ones, and the problems in NP are considered the "hard" ones
- The problems that are at least as hard as any other problem in NP and are in NP are called NP complete

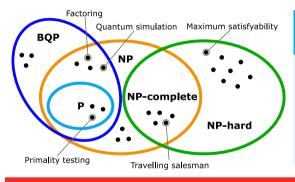


- P: decision problems solvable by a deterministic Turing machine in polynomial time
- NP: decision problems solvable by a non-deterministic Turing machine in polynomial time
 - Solution can be checked on a deterministic Turing machine in polynomial time
- Since an exponential function grows asymptotically faster than any polynomial problems in P are considered the "easy" ones, and the problems in NP are considered the "hard" ones
- The problems that are at least as hard as any other problem in NP and are in NP are called NP complete



BQP (bounded-error quantum polynomial time):

- Decision problems solvable by a quantum computer in polynomial time with error probability less than 1/3
- > Quantum equivalent to P, "easy problems"

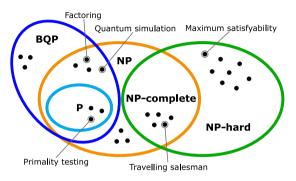


BQP (bounded-error quantum polynomial time):

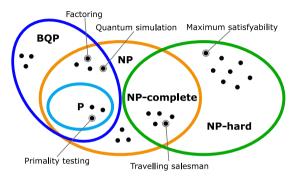
- Decision problems solvable by a quantum computer in polynomial time with error probability less than 1/3
- > Quantum equivalent to P, "easy problems"

Take home message

- > Exponential speedup on a quantum computer only for very specific problems
- No exponential speedup for NP-complete problems!



Not strictly proven, proving $P \neq NP$ is one of the millennium problems



- Not strictly proven, proving P ≠ NP is one of the millennium problems
- > If P = NP then quantum computers would not allow for an exponential speedup
- Empirically, nobody has found a polynomial time algorithm for (all instances of) a problem in NP

https://www.claymath.org/millennium-problems/

4.

The Deutsch-Josza algorithm

Grover's algorithm

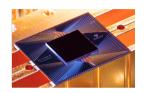
Complexity theory

Hybrid quantum-classical algorithms

Challenges for hybrid quantum-classical algorithms

On the verge of the NISQ era

- > Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible



J. Preskill, Quantum 2, 79 (2018)

On the verge of the NISQ era

- > Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers for "artificially tailored" tasks



J. Preskill, Quantum 2, 79 (2018) F. Arute et al., Nature 574, 5050 (2019)

On the verge of the NISQ era

- > Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers for "artificially tailored" tasks



Quantum supremacy using a programmable superconducting processor

Https://dei.org/10.3938/s41586-016-16 Received: 22 Ady 2019 Accepted: 20 September 2019 Debblook online: 33 October 2015

Article

QUANTUM COMPUTING

RESEARCH

Quantum computational advantage using photons

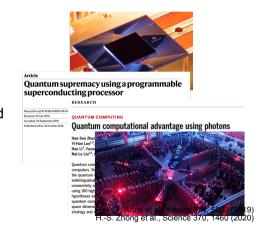
Han Sen Zhong^{1,2}*, Hui Wang^{1,2}*, Yu-Hao Deng^{1,2}*, Ming Cheng Chen^{1,2}*, Li Chao Peng^{1,2}*, I'Han Luo^{1,3}, Jian Qiu^{1,2}, Dian Wu^{1,2}, Xing Ding^{1,2} Yi Hu^{1,2}, Peng Hu^{1,2}, Xiao Yan Yang¹, Wei-Jun Zhang¹, Hao Li¹, Yuxuan (Yi, Xiao Jiang^{1,2}, Li Gan¹, Guangwen Yang¹, Lixing You¹, Zhen Wang¹, Li Li^{1,2}*, Nai-Le Liu^{1,2}*, Chao-Yang Lu^{2,2}*, Jian-Wei Pan^{1,2}*, I

Quarban comparies promise to perform certain tasks that are believed to be intractable to classical comparies. Boom sampling is such at task and is considered at storm candidate to demonstrated the quantum computational advantage. We performed Guarsian boom sampling by sending 50 most provided to the provided of the

F. Arute et al., Nature 574, 5050 (2019) H.-S. Zhong et al., Science 370, 1460 (2020)

On the verge of the NISQ era

- > Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers for "artificially tailored" tasks



On the verge of the NISQ era

- > Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers for "artificially tailored" tasks
- For certain simple models NISQ devices results were comparable with state of the art methods

Article

Evidence for the utility of quantum computing before fault tolerance

https://doi.org/10.1038/s41586-023-06096-3 Received: 24 February 2023 Accepted: 18 April 2023 Published online: 14 June 2023 Open access

Open access

Check for updates

Youngseok Kim^{**II}, Andrew Eddins^{3,1 II}, Sajant Anand³, Ken Xuan Wei¹, Ewout van den Berg¹, Sami Rosenblatt¹, Hasan Nayfeh¹, Yantao Wu^{3,4}, Michael Zaletel^{1,5}, Kristan Temme¹ & Abhinav Kandala^{1,1}

Quantum computing promises to offer substantial speed-ups over its classical counterpart for certain problems. However, the greatest impediment to realizing its full potential is poise that is inherent to these systems. The widely accented solution to this challenge is the implementation of fault-tolerant quantum circuits, which is out of reach for current processors. Here we report experiments on a noisy 127-qubit processor and demonstrate the measurement of accurate expectation values for circuit volumes at a scale beyond brute force classical computation. We armue that this represents evidence for the utility of quantum computing in a pre-fault-tolerant era. These experimental results are enabled by advances in the coherence and calibration of a superconducting processor at this scale and the ability to characterize and controllably manipulate noise across such a large device. We establish the accuracy of the measured expectation values by comparing them with the output of exactly verifiable circuits. In the regime of strong entanglement, the quantum computer provides correct results for which leading classical approximations such as pure-state based 1D (matrix product states, MPS) and 2D (isometric tensor network states isoTNS) tensor network methods 1.3 break down. These experiments demonstrate a foundational tool for the realization of near-term quantum applications 4.5.

F. Arute et al., Nature 574, 5050 (2019) H.-S. Zhong et al., Science 370, 1460 (2020) Y. Kim et al., Nature 618, 500 (2023)

On the verge of the NISQ era

- Noisy intermediate-scale quantum computers with $\mathcal{O}(100)$ qubits are already available
- Noise significantly limits the circuit depths that can be executed reliably, no quantum error correction possible
- Current NISQ devices have already outperformed classical computers for "artificially tailored" tasks
- > For certain simple models NISQ devices results were comparable with state of the art methods
- Larger quantum devices in the near future with error correction are announced future

Article

Evidence for the utility of quantum computing before fault tolerance

https://doi.org/10.1038/s41586-023-06096-3 Peceivari 24 February 2023 Accepted: 18 April 2023 Published online: 14 June 2023 Open access Check for updates

Youngseok Kim^(A)), Andrew Eddins^(A)), Sajant Anand¹, Ken Xuan Wei¹, Ewout van den Berg¹, Sami Bosenhiatti Hasan Navfehi Yantan Wulit Michael Zaleteilla Kristan Tamme' S Abhinay Kandala¹¹¹

Quantum computing promises to offer substantial speed-ups over its classical counterpart for certain problems. However, the greatest impediment to realizing its full potential is poise that is inherent to these systems. The widely accented solution to this challenge is the implementation of fault-tolerant quantum circuits, which is out of reach for current processors. Here we report experiments on a noisy 127-qubit processor and demonstrate the measurement of accurate expectation values for circuit volumes at a scale beyond brute force classical computation. We armue that this represents evidence for the utility of quantum computing in a pre-fault-tolerant era. These experimental results are enabled by advances in the coherence and calibration of a superconducting processor at this scale and the ability to characterize and controllably manipulate noise across such a large device. We establish the accuracy of the measured expectation values by comparing them with the output of exactly verifiable circuits. In the regime of strong entanglement, the quantum computer provides correct results for which leading classical approximations such as pure-state based 1D (matrix product states, MPS) and 2D (isometric tensor network states isoTNS) tensor network methods 1.3 break down. These experiments demonstrate a foundational tool for the realization of near-term quantum applications 4.5.

F. Arute et al., Nature 574, 5050 (2019)

H.-S. Zhong et al., Science 370, 1460 (2020) Y. Kim et al., Nature 618, 500 (2023) https://www.ibm.com/guantum/technology#scaling-guantum-computing.https://blog.google/technology/ai/unveiling-our-new-guantum-ai-campus/

Current NISQ devices

- > Small or intermediate scale
- Considerable amount of noise
- Only shallow circuits can be executed faithfully/no error correction
- Quantum advantage demonstrated

Current NISQ devices	Solving "useful" problems
 Small or intermediate scale Considerable amount of noise Only shallow circuits can be executed faithfully/no error correction Quantum advantage demonstrated 	 Large number of qubits Deep circuits Quantum error correction necessary So far only proof of principle demonstrations



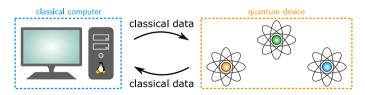


Current NISQ devices	Solving "useful" problems
> Small or intermediate scale	> Large number of qubits
Considerable amount of noise	> Deep circuits
> Only shallow circuits can be executed	> Quantum error correction necessary
faithfully/no error correction	> So far only proof of principle
> Quantum advantage demonstrated	demonstrations

How can we utilize existing quantum hardware in a beneficial way?

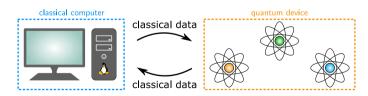
The basic idea of hybrid quantum-classical algorithms

- Combine classical and quantum devices
- > Rely on classical computing where possible
- > Use the quantum device as a coprocessor
 - Tackle the classically hard/intractable part of the problem
 - Feed the classical data obtained from a measurement back to the classical computer



The basic idea of hybrid quantum-classical algorithms

- Combine classical and quantum devices
- > Rely on classical computing where possible
- > Use the quantum device as a coprocessor
 - Tackle the classically hard/intractable part of the problem
 - Feed the classical data obtained from a measurement back to the classical computer



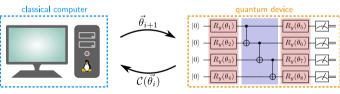
Even modest quantum hardware can yield advantages

Variational quantum-classical algorithms

> Focus on optimization problems trying to minimize a cost function $\mathcal{C}(\vec{\theta})$

$$\min_{\vec{\theta}} \mathcal{C}(\vec{\theta}) = \langle \psi(\vec{\theta}) | H | \psi(\vec{\theta}) \rangle, \qquad \vec{\theta} = \mathbb{R}^n$$

- > Solve them iteratively using a parametric ansatz
 - Quantum coprocessor: prepare the **variational ansatz** $|\psi(\vec{\theta_i})\rangle$ and evaluate $\mathcal{C}(\vec{\theta_i})$
 - Classical computer: given $\mathcal{C}(\vec{\theta_i})$, find optimized $\vec{\theta}_{i+1}$

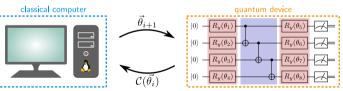


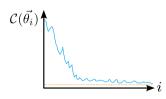
Variational quantum-classical algorithms

> Focus on optimization problems trying to minimize a cost function $\mathcal{C}(\vec{\theta})$

$$\min_{\vec{\theta}} \mathcal{C}(\vec{\theta}) = \langle \psi(\vec{\theta}) | H | \psi(\vec{\theta}) \rangle, \qquad \vec{\theta} = \mathbb{R}^n$$

- > Solve them iteratively using a parametric ansatz
 - Quantum coprocessor: prepare the **variational ansatz** $|\psi(\vec{\theta}_i)\rangle$ and evaluate $\mathcal{C}(\vec{\theta}_i)$
 - Classical computer: given $\mathcal{C}(\vec{\theta_i})$, find optimized $\vec{\theta}_{i+1}$

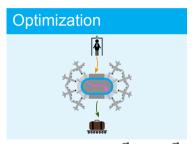


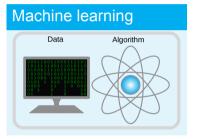


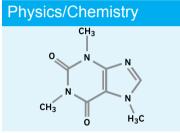
Run feedback loop between the classical computer and the quantum device until convergence

Why variational quantum algorithms?

> A large class of problems is naturally of that form or can be recast into such a form





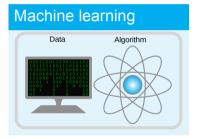


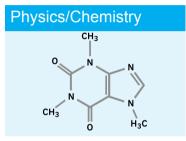
> Evaluating $\langle \psi(\vec{\theta})|H|\psi(\vec{\theta})\rangle$ is in general exponentially costly on classical computers

Why variational quantum algorithms?

> A large class of problems is naturally of that form or can be recast into such a form

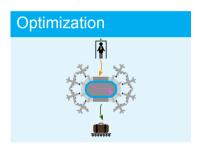
Optimization

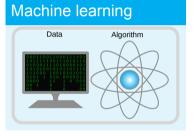


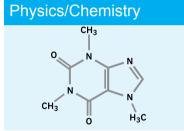


- > Evaluating $\langle \psi(\vec{\theta})|H|\psi(\vec{\theta})\rangle$ is in general exponentially costly on classical computers
- > Given that the ansatz $|\psi(\vec{ heta})
 angle$ is expressive enough at the end of the optimization
 - $\mathcal{C}(ec{ heta})$ corresponds to the smallest eigenvalue E_0 of H
 - = $|\psi(\vec{ heta})
 angle$ is the corresponding eigenstate, i.e. the ground state of H

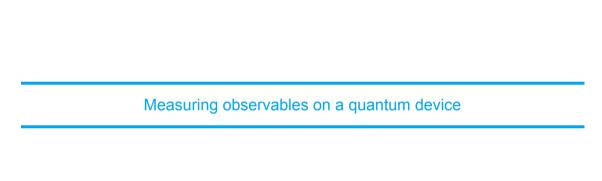
How to implement variational quantum algorithms?







- > How do we measure the cost function?
- > How can we cast problems in such a form?
- How can we choose a suitable ansatz?



Measuring observables

- > Given an observable O we want to compute $\langle \psi | O | \psi \rangle$
- > State can only be measured in the computational basis

$$\langle \psi | O | \psi \rangle = \langle \psi | U^{\dagger} U O U^{\dagger} U | \psi \rangle = \langle \psi' | U O U^{\dagger} | \psi' \rangle = \langle \psi' | D | \psi' \rangle$$

Measuring observables

- > Given an observable O we want to compute $\langle \psi | O | \psi \rangle$
- > State can only be measured in the computational basis

$$\left\langle \psi\right|O\left|\psi\right\rangle = \left\langle \psi\right|U^{\dagger}UOU^{\dagger}U\left|\psi\right\rangle = \left\langle \psi'\right|UOU^{\dagger}\left|\psi'\right\rangle = \left\langle \psi'\right|D\left|\psi'\right\rangle$$

- > Choose U such that $D=UOU^\dagger=\mathrm{diag}(\lambda_0,\dots,\lambda_{2^N-1})=\sum_x\lambda_x\,|x\rangle\langle x|$ in the computational basis
- > Expand $|\psi'\rangle$ in the computational basis: $|\psi'\rangle = \sum_x c_x' |x\rangle$

$$\left\langle \psi \right| O \left| \psi \right\rangle = \left\langle \psi' \right| D \left| \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \lambda_{x} \left\langle \psi' \underbrace{\left| x \right\rangle \left\langle x \right|}_{P_{x}} \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \lambda_{x} \left\langle \psi' \middle| P_{x} \middle| \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \left| c_{x}' \middle|^{2} \lambda_{x} \right|$$

Measuring observables

- > Given an observable O we want to compute $\langle \psi | O | \psi \rangle$
- > State can only be measured in the computational basis

$$\left\langle \psi\right|O\left|\psi\right\rangle = \left\langle \psi\right|U^{\dagger}UOU^{\dagger}U\left|\psi\right\rangle = \left\langle \psi'\right|UOU^{\dagger}\left|\psi'\right\rangle = \left\langle \psi'\right|D\left|\psi'\right\rangle$$

- > Choose U such that $D=UOU^\dagger=\mathrm{diag}(\lambda_0,\ldots,\lambda_{2^N-1})=\sum_x\lambda_x\,|x\rangle\langle x|$ in the computational basis
- > Expand $|\psi'\rangle$ in the computational basis: $|\psi'\rangle = \sum_x c_x' \, |x\rangle$

$$\left\langle \psi \right| O \left| \psi \right\rangle = \left\langle \psi' \right| D \left| \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \lambda_{x} \left\langle \psi' \underbrace{\left| x \right\rangle \left\langle x \right|}_{P_{x}} \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \lambda_{x} \left\langle \psi' \middle| P_{x} \middle| \psi' \right\rangle = \sum_{x=0}^{2^{N}-1} \left| c_{x}' \middle|^{2} \lambda_{x} \right|$$

- U is often called post rotation
- > Instead of $|\psi\rangle$ we prepare $|\psi'\rangle$ and measure the probability distribution $|c_x'|^2$

Example

- > State $|\psi\rangle = R_y(\pi/4) |0\rangle$
- ightharpoonup Observable we want to measure O=X

$$D = UOU^{\dagger} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= HXH = Z$$

$$|\psi'\rangle = U |\psi\rangle = HR_y(\pi/4) |0\rangle$$

$$|0\rangle - R_y(\pi/4) - H$$

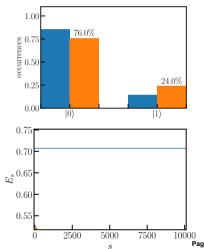
Example

- > State $|\psi\rangle = R_y(\pi/4) |0\rangle$
- ightharpoonup Observable we want to measure O=X

$$D = UOU^{\dagger} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= HXH = Z$$

$$|\psi'\rangle = U |\psi\rangle = HR_y(\pi/4) |0\rangle$$

$$|0\rangle - R_y(\pi/4) - H$$



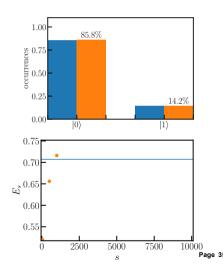
Example

- > State $|\psi\rangle = R_y(\pi/4) |0\rangle$
- ightharpoonup Observable we want to measure O=X

$$D = UOU^{\dagger} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= HXH = Z$$

$$|\psi'\rangle = U |\psi\rangle = HR_y(\pi/4) |0\rangle$$

$$|0\rangle - R_y(\pi/4) - H$$



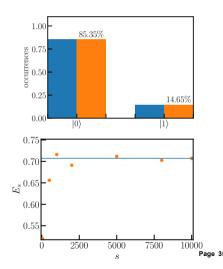
Example

- > State $|\psi\rangle = R_y(\pi/4) |0\rangle$
- ightharpoonup Observable we want to measure O=X

$$D = UOU^{\dagger} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= HXH = Z$$

$$|\psi'\rangle = U |\psi\rangle = HR_y(\pi/4) |0\rangle$$

$$|0\rangle - R_y(\pi/4) - H$$



Example

- > State $|\psi\rangle = R_y(\pi/4) |0\rangle$
- ightharpoonup Observable we want to measure O=X

$$D = UOU^{\dagger} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} X \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= HXH = Z$$

> Circuit to prepare and measure

$$|\psi'\rangle = U |\psi\rangle = HR_y(\pi/4) |0\rangle$$

$$|0\rangle - R_y(\pi/4) - H$$

 \Rightarrow Error is $\propto 1/\sqrt{s} \rightarrow 0$ for $s \rightarrow \infty$

Quantum Approximate Optimization Algorithm (QAOA)

Combinatorial optimization problems

> Algorithm for approximating (binary) combinatorial optimization problems

$$\min_{x \in V} C(x)$$
 subject to $x \in S$

- > x: binary string in $V = \{0, 1\}^n$ encoding a solution
- > $S \subseteq V$: feasible solutions
- $> C: V \rightarrow \mathbb{R}$ cost function
- > Objective is to find the optimal solution

The Max-Cut problem

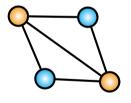
Max-Cut

- **Input:** undirected graph G = (V, E)
- > Task: find a bipartition of $V = A \cup B$ such that the number of edges between A and B is maximal

The Max-Cut problem

Max-Cut

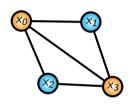
- **Input:** undirected graph G = (V, E)
- **> Task:** find a bipartition of $V = A \cup B$ such that the number of edges between A and B is maximal
- Max-Cut is NP-complete
- ⇒ We cannot find a (quantum) algorithm which solves it polynomial time
- We can however try to find a good approximation to the exact solution in polynomial time



Max-Cut as combinatorial optimization problem

- > Max-Cut on a Graph G=(V,E) can be expressed as combinatorial optimization problem
- > Label the vertices as x_i define a function w_{ij}

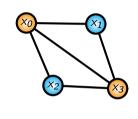
$$x_i = \begin{cases} 0 & \text{if } i \in A \\ 1 & \text{if } i \in B \end{cases}$$
 $w_{ij} = \begin{cases} 1 & \text{iff } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$



Max-Cut as combinatorial optimization problem

- > Max-Cut on a Graph G=(V,E) can be expressed as combinatorial optimization problem
- > Label the vertices as x_i define a function w_{ij}

$$x_i = \begin{cases} 0 & \text{if } i \in A \\ 1 & \text{if } i \in B \end{cases} \qquad w_{ij} = \begin{cases} 1 & \text{iff } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$



> Cost function

$$C(x) = \sum_{i,j=0}^{n-1} w_{ij} x_i(x_j - 1) = \sum_{(i,j) \in E} (x_i(x_j - 1) + x_j(x_i - 1))$$

- \Rightarrow Contribution of -1 iff endpoints of edge (i, j) belong to different subsets
- \rightarrow Finding the Max-Cut for G is equivalent to minimizing C(x)

Max-Cut as Hamiltonian problem

lacksquare Cost function can be turned into a Hamiltonian using the mapping $x_i o rac{1}{2}(1-Z_i)$

$$H_c = \frac{1}{2} \sum_{(i,j) \in E} (Z_i Z_j - 1)$$

Diagonal Hamiltonian of Ising type, summands commute

Max-Cut as Hamiltonian problem

> Cost function can be turned into a Hamiltonian using the mapping $x_i o rac{1}{2}(1-Z_i)$

$$H_c = \frac{1}{2} \sum_{(i,j) \in E} (Z_i Z_j - 1)$$





Diagonal Hamiltonian of Ising type, summands commute

Max-Cut as Hamiltonian problem

> Cost function can be turned into a Hamiltonian using the mapping $x_i o \frac{1}{2}(1-Z_i)$

$$H_c = \frac{1}{2} \sum_{(i,j) \in E} (Z_i Z_j - 1)$$







- Diagonal Hamiltonian of Ising type, summands commute
- lacktriangle The eigenstates of H are computational basis states which encode graph cuts
- > The lower the energy, the larger the number of edges between the subsets
- > The ground state $|x^*\rangle$ encodes the bit string of the optimal solution x^*

Max-Cut as Hamiltonian problem

> Cost function can be turned into a Hamiltonian using the mapping $x_i o \frac{1}{2}(1-Z_i)$

$$H_c = \frac{1}{2} \sum_{(i,j) \in E} (Z_i Z_j - 1)$$







- > Diagonal Hamiltonian of Ising type, summands commute
- ullet The eigenstates of H are computational basis states which encode graph cuts
- > The lower the energy, the larger the number of edges between the subsets
- > The ground state $|x^*\rangle$ encodes the bit string of the optimal solution x^*

How to choose a suitable ansatz to find a low energy state of H?

The Quantum Approximate Optimization Algorithm (QAOA)

> We want to find a parametric quantum state $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$, $\vec{\gamma}$, $\vec{\beta} \in \mathbb{R}^p$ which minimizes

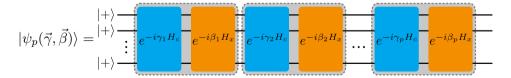
$$C(\vec{\gamma}, \vec{\beta}) = \langle \psi_p(\vec{\gamma}, \vec{\beta}) | H_c | \psi_p(\vec{\gamma}, \vec{\beta}) \rangle$$

The Quantum Approximate Optimization Algorithm (QAOA)

> We want to find a parametric quantum state $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$, $\vec{\gamma}$, $\vec{\beta} \in \mathbb{R}^p$ which minimizes

$$C(\vec{\gamma}, \vec{\beta}) = \langle \psi_p(\vec{\gamma}, \vec{\beta}) | H_c | \psi_p(\vec{\gamma}, \vec{\beta}) \rangle$$

- > Mixing Hamiltonian $H_x = \sum_i X_i$
- Ansatz structure



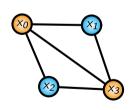
 $|+\rangle=rac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$ is an eigenstate of $X,X|+\rangle=+1|+\rangle$ E. Farhi, J. Goldstone, S. Gutmann, arXiv:1411.4028

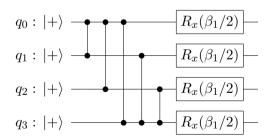
The Quantum Approximate Optimization Algorithm (QAOA)

> Ansatz for $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$

$$|\psi_p(\vec{\gamma}, \vec{\beta})\rangle = e^{-i\beta_p H_x} e^{-i\gamma_p H_c} \dots e^{-i\beta_1 H_x} e^{-i\gamma_1 H_c} |+\rangle^{\otimes n}$$

ightharpoonup Circuit for p=1

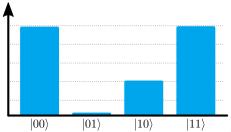




E. Farhi, J. Goldstone, S. Gutmann, arXiv:1411.4028

The Quantum Approximate Optimization Algorithm (QAOA)

- > $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$ is in general an (entangled) superposition of basis states
- > After minimizing $\mathcal{C}(\vec{\gamma}, \vec{\beta})$ the wave function $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$ has dominant component(s) of low energy states of H_c
- > Measuring $|\psi_p(\vec{\gamma}, \vec{\beta})\rangle$ reveals the a bit string(s) x corresponding to low energy states

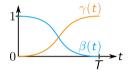


E. Farhi, J. Goldstone, S. Gutmann, arXiv:1411.4028

The Quantum Approximate Optimization Algorithm (QAOA)

- > Ansatz is inspired by trotterized adiabatic time evolution
- > Choose functions $\gamma(t)$, $\beta(t)$ such that

$$\gamma(t) o \begin{cases} 0 & \text{for } t o 0 \\ 1 & \text{for } t o T \end{cases} \qquad \beta(t) o \begin{cases} 1 & \text{for } t o 0 \\ 0 & \text{for } t o T \end{cases}$$



and set
$$\gamma_k = \gamma(k\Delta t)\Delta t$$
, $\beta_k = \beta(k\Delta t)\Delta t$

⇒ QAOA ansatz is a stroboscopbic version of the adiabatic evolution

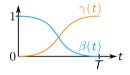
B. Barak et al., arXiv:2106.05900 E. Farhi, A. Harrow, arXiv:1602.07674

E. Farhi, J. Goldstone, S. Gutmann, arXiv:1411.4028 V. Akshav, H. Philathong, M. E. S. Morales, J. D. Biamonte, Phys. Rev. Lett 124, 090504 (2020)

The Quantum Approximate Optimization Algorithm (QAOA)

- > Ansatz is inspired by trotterized adiabatic time evolution
- > Choose functions $\gamma(t)$, $\beta(t)$ such that

$$\gamma(t) o \begin{cases} 0 & \text{for } t o 0 \\ 1 & \text{for } t o T \end{cases} \qquad \beta(t) o \begin{cases} 1 & \text{for } t o 0 \\ 0 & \text{for } t o T \end{cases} \qquad 0$$



and set
$$\gamma_k = \gamma(k\Delta t)\Delta t$$
, $\beta_k = \beta(k\Delta t)\Delta t$

- ⇒ QAOA ansatz is a stroboscopbic version of the adiabatic evolution
- ightharpoonup Even p=1 can in general not be simulated on a classical computer efficiently
- > For some problems classical algorithms got a better approximation ratios
- B. Barak et al., arXiv:2106.05900

 Theoretically it is not entirely clear how QAOA performs

 E. Farhi, J. Goldstone, S. Gutmann, arXiv:1402.07674

 V. Akshav, H. Philathona, M. E. S. Morales, J. D. Biamonte, Phys. Rev. Lett 124, 090504 (2020)

Variational Quantum Eigensolver (VQE)

Variational Quantum Algorithms

- > Same principle can be used to find ground states of general quantum Hamiltonians
- > Define a cost function

$$\mathcal{C}(\vec{\theta}) = \langle \psi(\vec{\theta}) | H | \psi(\vec{\theta}) \rangle$$

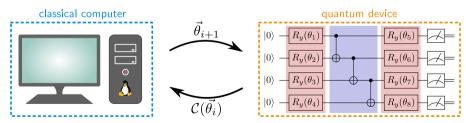
- > $|\psi(\vec{ heta})
 angle$ ansatz realized by a parametric quantum circuit
- In practice ansätze are often built by repeating a layered structure

Variational Quantum Algorithms

- > Same principle can be used to find ground states of general quantum Hamiltonians
- Define a cost function

$$\mathcal{C}(\vec{\theta}) = \langle \psi(\vec{\theta}) | H | \psi(\vec{\theta}) \rangle$$

- $> |\psi(\vec{\theta})\rangle$ ansatz realized by a parametric quantum circuit
- In practice ansätze are often built by repeating a layered structure



A. Peruzzo et al., Nat. Commun. 5, 1 (2014) J. R. McClean et al., New J. Phys. 18, 023023 (2016)

Variational Quantum Eigensolver (VQE)

> To measure a general N-qubit Hamiltonian, we translate it into a sum of Pauli terms

$$H = \sum_{i} c_i P_i$$

with $P_i \in \{\mathbb{1}, X, Y, Z\}^{\otimes N}$ a Pauli string and real coefficients c_i

This can always be done, as the Pauli matrices form a basis for the real vector space of Hermitian matrices (see exercises)

Variational Quantum Eigensolver (VQE)

> To measure a general N-qubit Hamiltonian, we translate it into a sum of Pauli terms

$$H = \sum_{i} c_i P_i$$

with $P_i \in \{\mathbb{1}, X, Y, Z\}^{\otimes N}$ a Pauli string and real coefficients c_i

- This can always be done, as the Pauli matrices form a basis for the real vector space of Hermitian matrices (see exercises)
- > The cost function is then given by

$$C(\vec{\theta}) = \sum_{i} c_i \langle \psi(\vec{\theta}) | P_i | \psi(\vec{\theta}) \rangle$$

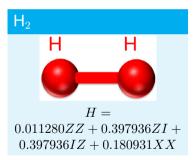
- > The individual terms $\langle \psi(\vec{\theta})|P_i|\psi(\vec{\theta})\rangle$ can be measured as discussed before
- \Rightarrow This is efficient as long there is only on number of $\mathcal{O}(\mathsf{poly}(N))$ terms with

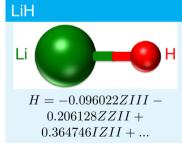
nonvanishing coefficients in H

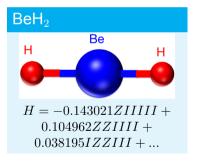
J. R. McClean et al., New J. Phys. 18, 023023 (2016) A. Peruzzo et al., Nat. Commun. 5, 1 (2014)

Example: VQE for molecules

> Use the VQE for finding the potential energy surface of molecules

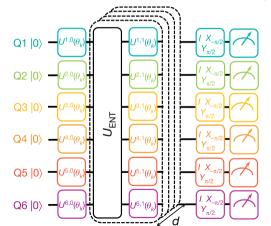






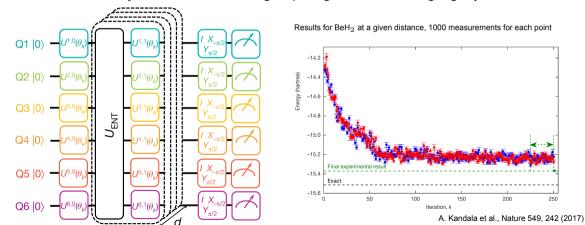
Example: VQE for molecules

> Ansatz circuit: layered structure of single-qubit gates and entangling layers



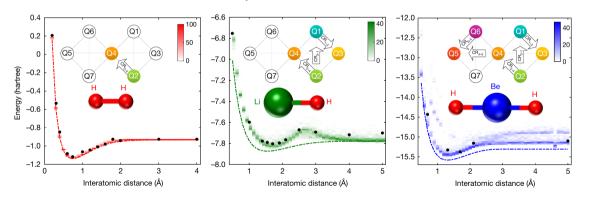
Example: VQE for molecules

> Ansatz circuit: layered structure of single-qubit gates and entangling layers



Example: VQE for molecules

> Results from the VQE for d = 1 layer of the ansatz



A. Kandala et al., Nature 549, 242 (2017)

QAQA

- > Combinatorial optimization problems
- Problem Hamiltonian is diagonal in the computational basis
- Circuit structure is fixed
- In the limit of infinite layers provably converges to the exact solution

Combinatorial optimization problems Problem Hamiltonian is diagonal in the computational basis Circuit structure is fixed In the limit of infinite layers provably converges to the exact solution Combinatorial optimization problems Ground states/low-lying excitations Efficient as long as H has only a polynomial number of terms Hamiltonian exists only as a measurement Great freedom choosing the circuit

Problem requirementsAvailable hardwareExpressiveness

QAQA VQE Combinatorial optimization problems Ground states/low-lying excitations Problem Hamiltonian is diagonal in the > Efficient as long as H has only a polynomial number of terms computational basis Circuit structure is fixed Hamiltonian exists only as a measurement In the limit of infinite lavers provably Great freedom choosing the circuit converges to the exact solution Problem requirements Available hardware Expressiveness

- Best answer for the given set of resources
- > Largely resilient to systematic errors of the device

Remarks on VQE and QAOA

- QAOA can be seen as specific type of ansatz for the VQE
- Although QAOA was originally developed for combinatorial optimization problems it can be applied to arbitrary Hamiltonians

Remarks on VOE and QAQA

- > QAOA can be seen as specific type of ansatz for the VQE
- Although QAOA was originally developed for combinatorial optimization problems it can be applied to arbitrary Hamiltonians

J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, Nat. Commun. 9, 4812 (2018).
A. Arrasmith, M. Cerezo, P. Czarnik, L. Cincio, P. J. Coles, Quantum 5, 558 (2022).
A. Arrasmith, Z. Holmes, M. Cerezo, P. J. Coles, Quantum Science and Technology 7, 045015 (2022).

5.

The Deutsch-Josza algorithm

Grover's algorithm

Complexity theory

Hybrid quantum-classical algorithms

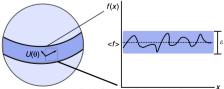
Challenges for hybrid quantum-classical algorithms

Barren plateaus

- > Optimizing the parameters using a classical algorithms turns out to be challenging
- For a wide class of parametrized circuits the probability to have a non-vanishing gradient along any direction vanishes exponentially with the number of qubits
- ⇒ Barren plateaus, gradient-based optimizers will fail

Barren plateaus

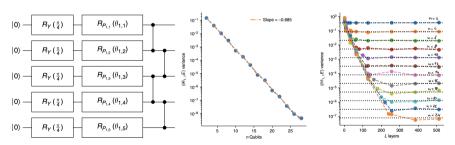
- > Optimizing the parameters using a classical algorithms turns out to be challenging
- For a wide class of parametrized circuits the probability to have a non-vanishing gradient along any direction vanishes exponentially with the number of qubits
- ⇒ Barren plateaus, gradient-based optimizers will fail
- Mathematical reason: concentration of measure, sufficiently smooth function is concentrated in an exponentially small region around the mean



J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, Nat Commun 9, 4812 (2018)

Barren plateaus

- This happens for sufficiently random circuits (match the Haar distribution up to the second moment)
- In practice this phenomena is already observed for relative simple ansatz circuits



J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, Nat Commun 9, 4812 (2018)

Barren plateaus

- It was shown that not only does the gradient vanish, but also the cost function has exponentially narrow minima
- Not only the gradients vanish exponentially, but also the variance of the cost function itself
- Switching to a gradient free optimization algorithm does not avoid the problem

Causes for barren plateaus

Ansätze that are too expressive in a sense that they are able to relatively how uniformly it explores the unitary space exhibit barren plateaus

Z. Holmes et al., PRX Quantum 3, 010313 (2022); J. Tangpanitanon et al., Phys. Rev. Research 2, 043364 2020

Causes for barren plateaus

- Ansätze that are too expressive in a sense that they are able to relatively how uniformly it explores the unitary space exhibit barren plateaus
- Circuits that generate a lot of entanglement (e.g. satisfying the volume law) exhibit barren plateaus

Z. Holmes et al., PRX Quantum 3, 010313 (2022); J. Tangpanitanon et al., Phys. Rev. Research 2, 043364 2020 C. Ortiz Marrero et al., PRX Quantum 2, 040316 (2021); T. L. Patti et al., Phys. Rev. Research 3, 033090 (2021); K. Sharma et al., Phys. Rev. Lett. 128 180505 (2022)

Causes for barren plateaus

- Ansätze that are too expressive in a sense that they are able to relatively how uniformly it explores the unitary space exhibit barren plateaus
- Circuits that generate a lot of entanglement (e.g. satisfying the volume law) exhibit barren plateaus
- Nature of the cost function, global cost functions are introducing barren plateaus, local cost functions only after a depth polynomial in the number of qubits

Z. Holmes et al., PRX Quantum 3, 010313 (2022); J. Tangpanitanon et al., Phys. Rev. Research 2, 043364 2020 C. Ortiz Marrero et al., PRX Quantum 2, 040316 (2021); T. L. Patti et al., Phys. Rev. Research 3, 033090 (2021); K. Sharma et al., Phys. Rev. Lett. 128 180505 (2022) M. Cerezo et al., Nat. Commun. 12, 1791, (2021)

Causes for barren plateaus

- Ansätze that are too expressive in a sense that they are able to relatively how uniformly it explores the unitary space exhibit barren plateaus
- Circuits that generate a lot of entanglement (e.g. satisfying the volume law) exhibit barren plateaus
- > Nature of the cost function, **global cost functions** are introducing barren plateaus, local cost functions only after a depth polynomial in the number of qubits
- Noise in the quantum device can wash out the features of the energy landscape leading to barren plateaus

Z. Holmes et al., PRX Quantum 3, 010313 (2022); J. Tangpanitanon et al., Phys. Rev. Research 2, 043364 2020 C. Ortiz Marrero et al., PRX Quantum 2, 040316 (2021); T. L. Patti et al., Phys. Rev. Research 3, 033090 (2021); K. Sharma et al., Phys. Rev. Lett. 128 180505 (2022)

M. Cerezo et al., Nat. Commun. 12, 1791, (2021) S. Wang et al., Nat. Commun. 12, 6961 (2021); D. Stilck Franca, R. García-Patrón, Nat. Phys. 17, 1221 (2021)

Avoiding/mitigating barren plateaus

- If possible, one can avoid the causes of barren plateaus, however this does not necessarily result in a trainable ansatz
- There is a plethora of proposals how to avoid/mitigate barren plateaus
 - Using modified cost functions

A. Wu, G. Li, Y. Ding, Y. Xie, arXiv:211:13209

Special choices of the initial variational parameters

Z. Holmes et al., PRX Quantum 3, 010313 (2022) K. Zhang et al., arXiv2203:09376

 Monitoring the entanglement during a gradient descent optimization in small subregions and adapting to learning rate to avoid uncontrolled entanglement growth

S. H. Sack et al., PRX Quantum 3, 020365 (2022)

. . . .

So far it seems that there is not simple way to avoid barren plateaus!

Thank you for your attention!

Further reading

- M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information, Cambridge university press (2010)
- J. R. McClean, J. Romero, R. Babbush, A. A. Guzik, New J. Phys. 18, 023023 (2016)
- > J. Tilly et al., Physics Reports **986**, 1-128 (1011)
- > https://learning.quantum-computing.ibm.com/



Contact

DESY. Deutsches Elektronen-Synchrotron

https://quantum-zeuthen.desy.de

Stefan Kühn

0000-0001-7693-350X
CQTA
stefan.kuehn@desy.de
+49 (0)33762 7-7288