Introduction to Quantum Algorithms

IQM Winter Quantum School – Day 2

Authors: Daniel Bulmash, Stefan Seegerer, Nadia Milazzo

Last Updated 11/2025

What’s an algorithm?

Problem

Sort a list of n numbers.

Instance

Sort this list of numbers:

18	42	-6	25	3	-8

An algorithm is a sequence of steps to solve a problem. Ideally, an algorithm should always solve the problem correctly no matter what instance you put in.

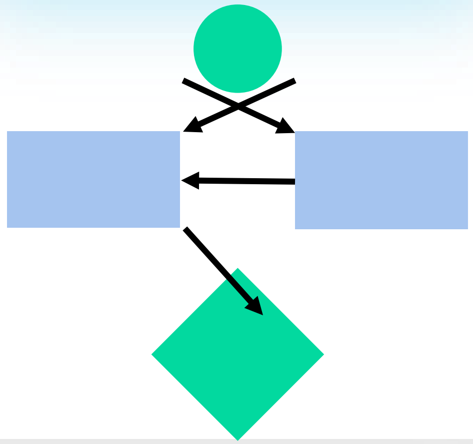
Classical algorithms

Prepare input

10110101001

Prepare a set of bits as input.

Apply logic



Perform a set of steps that transform the input into the problem solution.

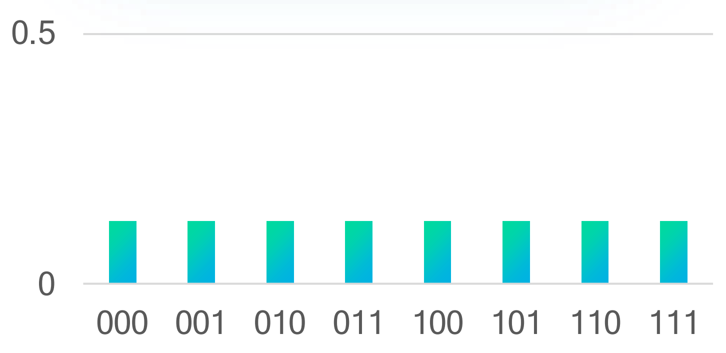
Measure outcome

00101100100

Read out the outcome.

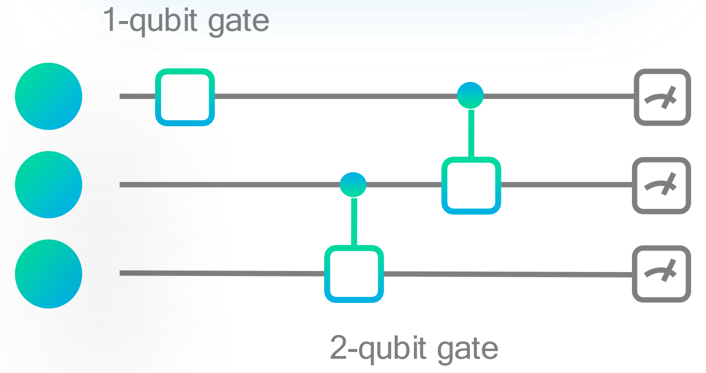
Quantum algorithms

Prepare state



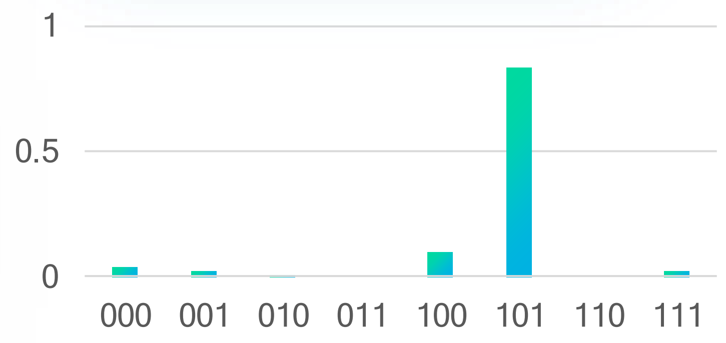
Use superposition/quantum parallelism to “process all possible inputs at once”

Apply circuit



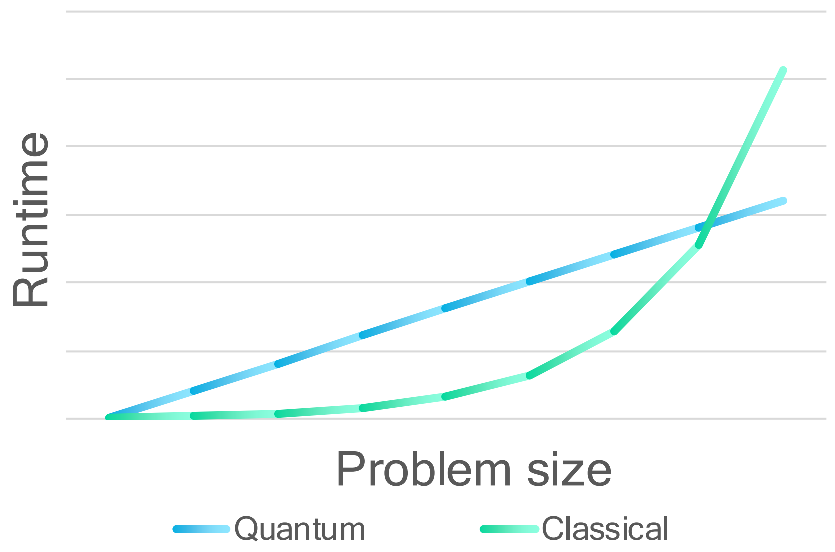
Use interference to make wanted outcomes more likely

Measure outcomes



Measure multiple times to find the most probable outcome

Quantum vs. classical



Quantum computers provide new algorithms that can be exponentially faster than classical computers at certain tasks, including simulation, optimization, or machine learning.

The landscape of quantum algorithms

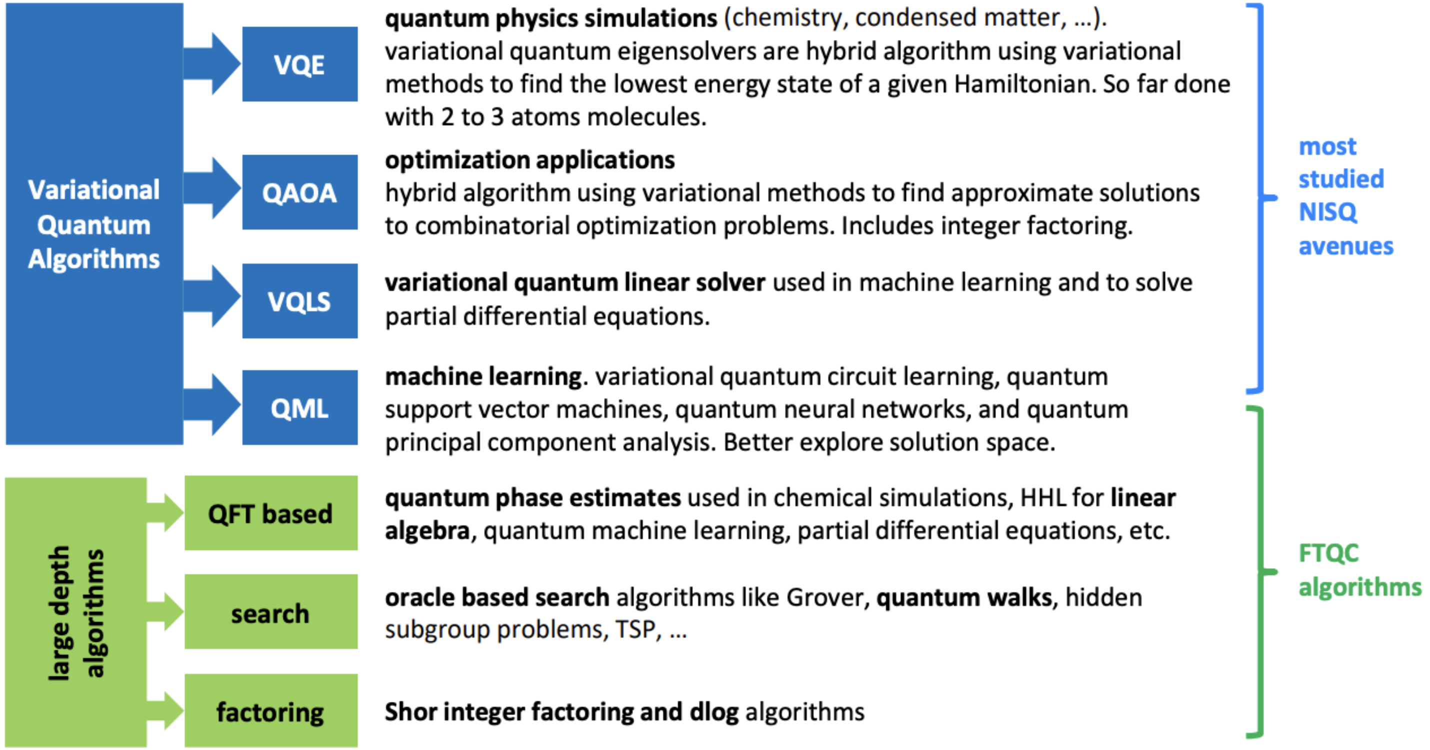


Figure 772 : the main NISQ algorithms classes as proposed by researchers and industry vendors, in blue, when those in green are specific to fault-tolerant quantum computers relying on quantum error correction. These NISQ variational algorithms should be theoretically resilient to noise and shallow but so far, they are not, particularly in a quantum advantage regime with over 50 qubits and with their current algorithm depth actual requirements. VQE algorithms scale in depth as N^6, N being their qubit numbers. Some proposed NISQ algorithms, not shown here, do not use a variational mechanism and may work better than variational algorithms. (cc) Olivier Ezratty, 2023.

Source: Olivier Ezratty (2023, Understanding Quantum Technologies)

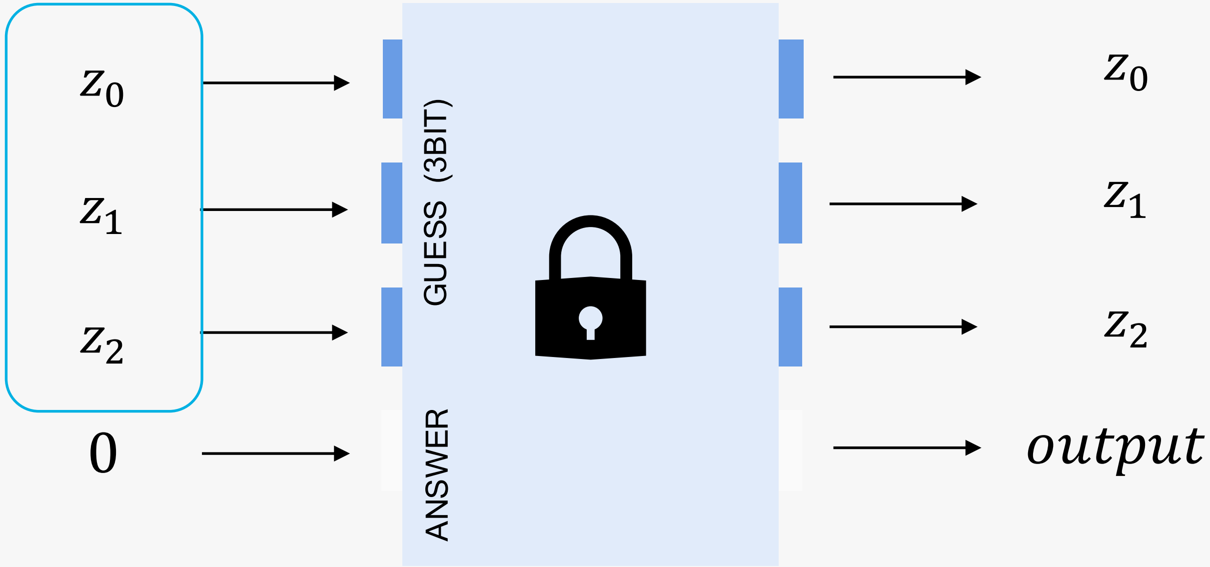
Outline for today

1. The Bernstein-Vazirani algorithm: a quantum algorithm that is provably better than any classical one
   - See how quantum parallelism and interference work
2. Variational quantum algorithms
   - QAOA: A classical-quantum hybrid algorithm that may be useful in the short term
3. Lab: Implement Bernstein-Vazirani and try using QAOA

A Simple Quantum Algorithm: Bernstein-Vazirani

Problem

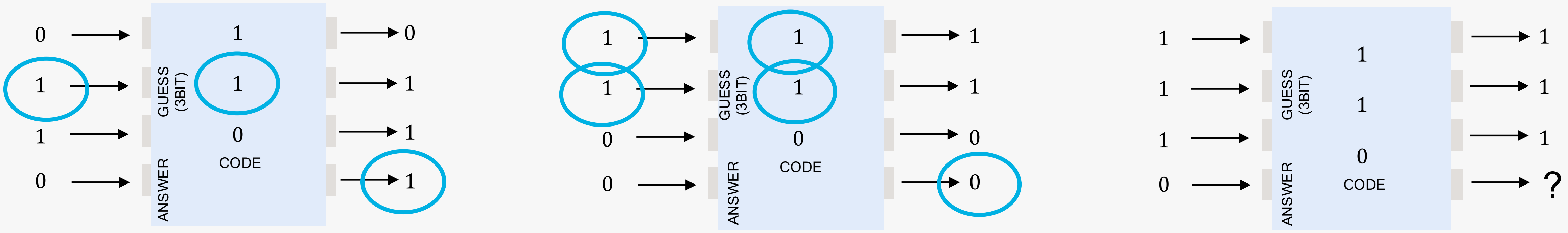
- Given: A secret (but unknown) code of n bits
- Given: A black box or "oracle"
  - Input: n "guess" qubits and one "answer" qubit
  - Oracle looks at the input and compares it to the secret code.
    - Every time a 1 in the guess matches a 1 in the code, it flips the answer qubit (0 → 1, 1 → 0)
  - Outputs the answer qubit, doesn't change the input qubits.
- **Goal**: identify secret code by experimenting with the oracle.



(Imagine a friend of ours made the oracle but didn't tell us the code.)

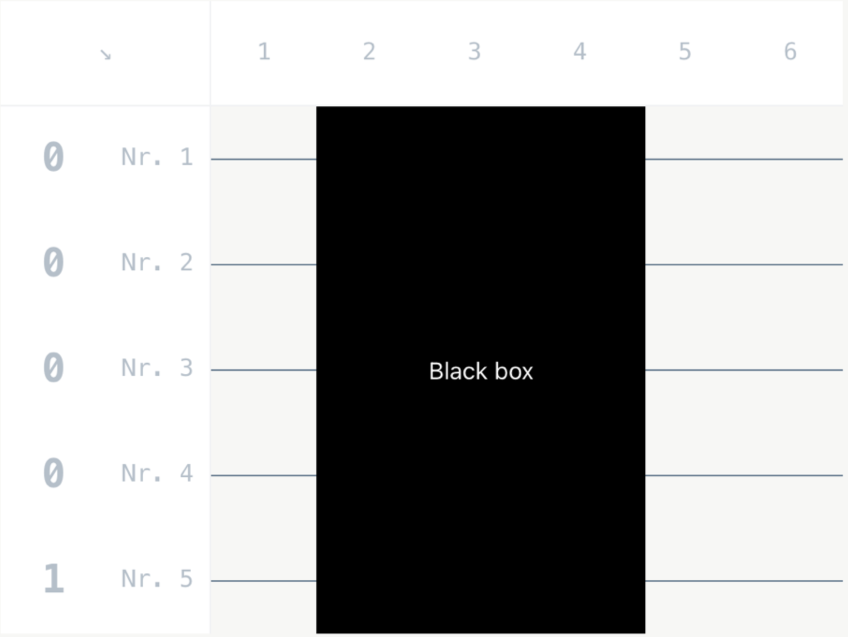
Example

Imagine the secret code is 110.



Experiment time!

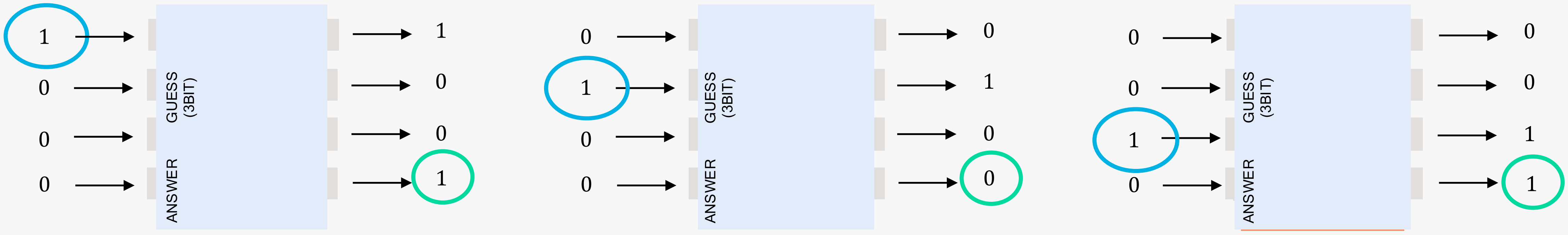
Use the applet here https://tinyurl.com/iqm-secret-code or the QR code to develop a strategy for finding the secret code. How many attempts do you need to find the code? Describe your approach.



IQM

One solution

- Set one input to 1 and the rest to 0.
- The last qubit indicates if there is a 0 or 1 on this position in the secret code
- Repeat for every digit in the secret code
- With this algorithm, we need to use the oracle n times to find the code c.
  - One can **prove** that no classical algorithm will use the oracle fewer than n times.

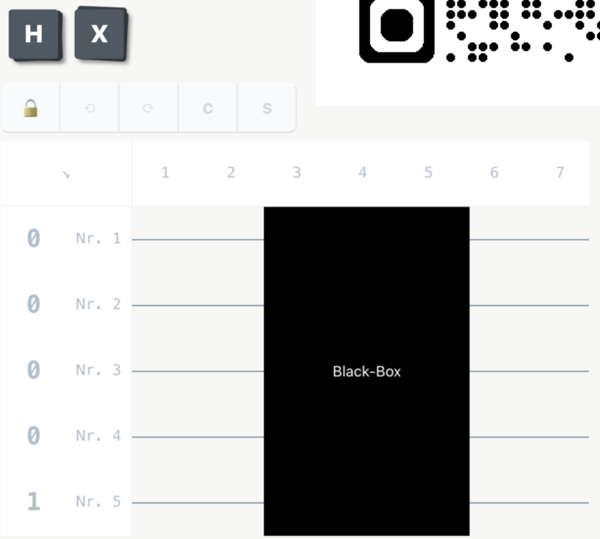


Secret code is: 101 !

Experiment time!

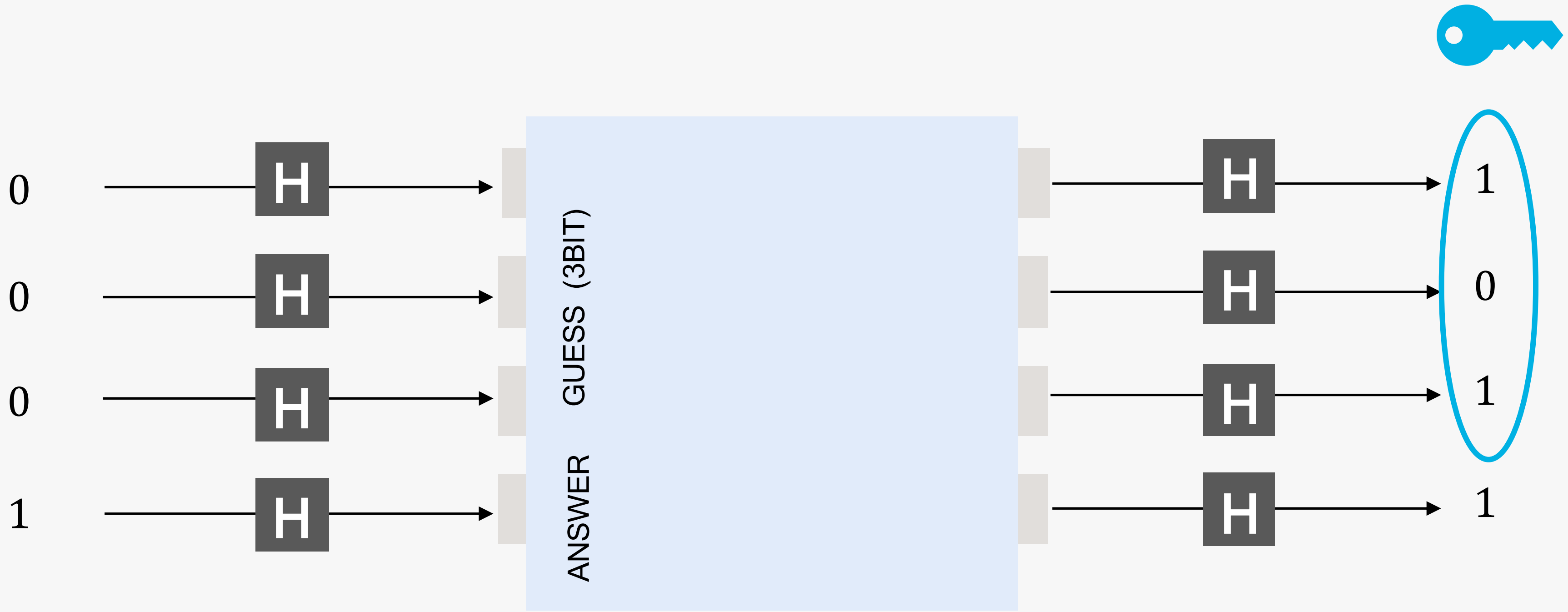
Explore the quantum solution with the applet https://tinyurl.com/iqm-solver ! To find out the secret 4-digit code of this black box, prepare an equal superposition of all 5 qubits. Also apply a set of **H** after the black box.

Afterward, open the black box and check how you can retrieve the secret code from the measurement outcomes.



Quantum solution – Bertstein-Vazirani algorithm

- Initialize guess qubits with 0, answer qubit with 1
- Apply H gates before and after the black box
- Output of guess qubits is the secret code 🤩



IQM

Attendance

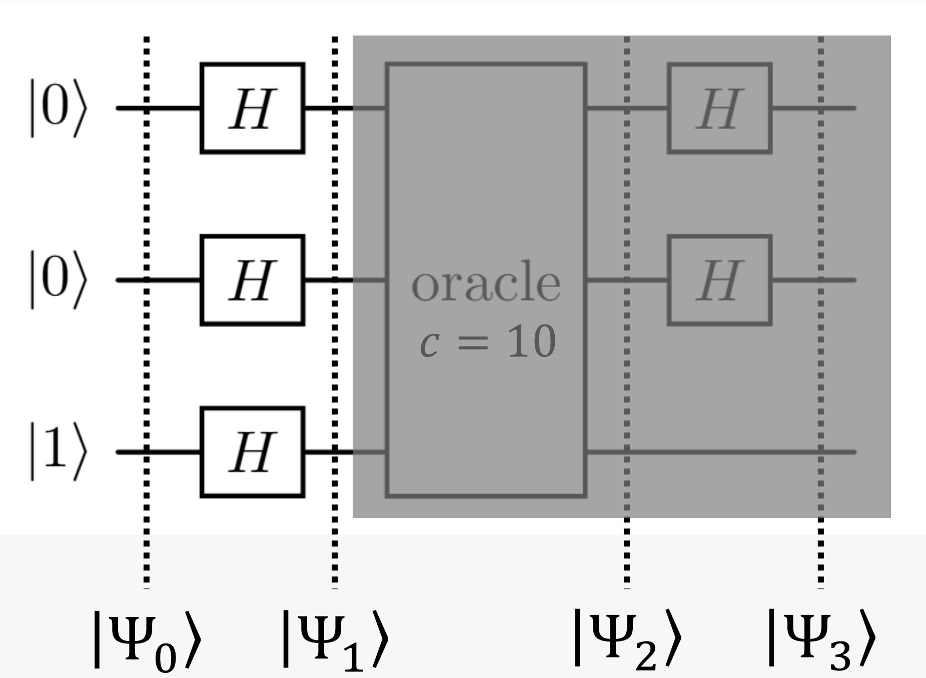
https://docs.google.com/forms/d/e/1FAIpQLScWEpHbVuHWutEXxBGh0IQaFx9OH2K6sbrDQs06v8f
eWD66WA/viewform?usp=dialog

IQM

How does Bernstein-Vazirani work?

Step 1: Quantum Parallelism

- The Bernstein-Vazirani algorithm finds c with a single query of f using interference and quantum parallelism.
- Let's see how this works for a 2-qubit example, where $c = 10$.



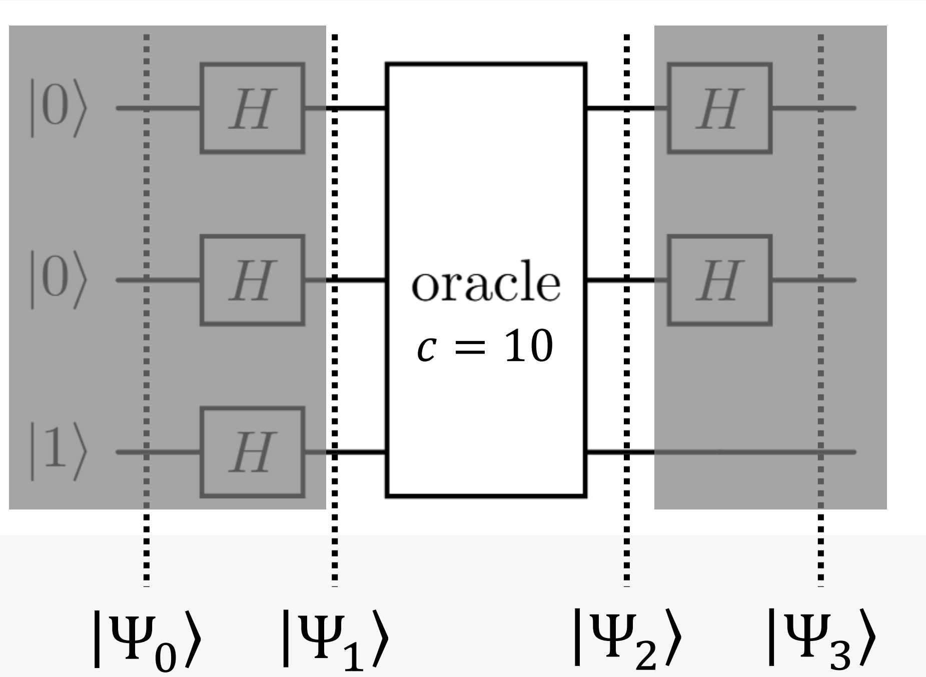
- $|\Psi_0\rangle = |00\rangle|1\rangle$
- $|\Psi_1\rangle = \frac{1}{\sqrt{2^2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$= \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- The H gates make it look like we "put in all possible inputs in parallel"

IQM

Step 2: Phase kickback



$$|\Psi_1\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Now apply the oracle. Let's look at some terms:
  - $\frac{1}{\sqrt{2^2}}|00\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2^2}}|00\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  - $\frac{1}{\sqrt{2^2}}|11\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2^2}}|11\rangle\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle)$

$$= \frac{1}{\sqrt{2^2}}(-|11\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

These minus signs can't happen for classical bits!

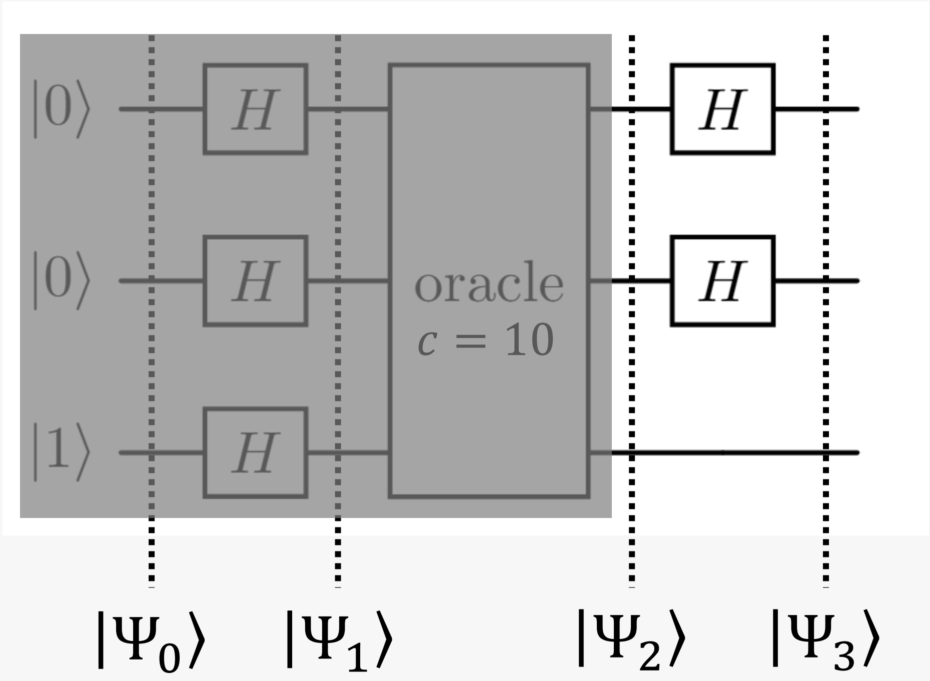
- So,

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The pattern of minus signs is determined by the secret code. This is called "phase kickback".

IQM

Step 3: Interference

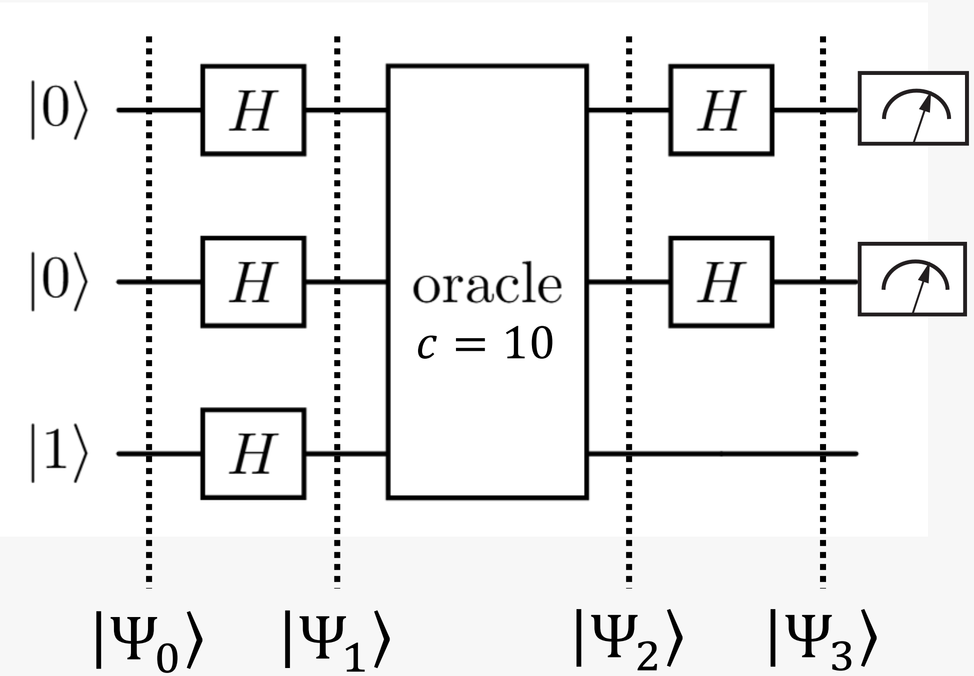


- $|\Psi_3\rangle = (H \otimes H \otimes I)|\Psi_2\rangle$
  $= \frac{1}{\sqrt{2^2}}(H \otimes H)(|00\rangle + |01\rangle - |10\rangle - |11\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Lots of output terms. You can check:
  - $(H \otimes H)|00\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
  - $(H \otimes H)|01\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).$
  - $-(H \otimes H)|10\rangle = -\frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle - |10\rangle - |11\rangle).$
  - $-(H \otimes H)|11\rangle = -\frac{1}{\sqrt{2^2}}(|00\rangle - |01\rangle - |10\rangle + |11\rangle).$

- Add up all the terms to get $|\Psi_3\rangle$:
  - Count the minus signs carefully. Two + and two - for every output… *except* for $|10\rangle$, which is all +!
- All possible outputs $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|x\rangle$ cancel out unless $|x\rangle = |c\rangle$, in which case they add up. This phenomenon is interference.

IQM

Bernstein-Vazirani algorithm - result



- $|\Psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|c\rangle.$
- A single measurement of the n qubits reveals the code c

What have we learned?

- Qubits leverage superposition to represent and process multiple states concurrently.

- This superposition, combined with entanglement, allows quantum algorithms to explore many possible solutions or paths in parallel within a single computation step.

- Quantum interference patterns are exploited to amplify correct solutions and suppress incorrect ones.

- These effects enable speedups compared to classical solutions.

Variational Quantum Algorithms

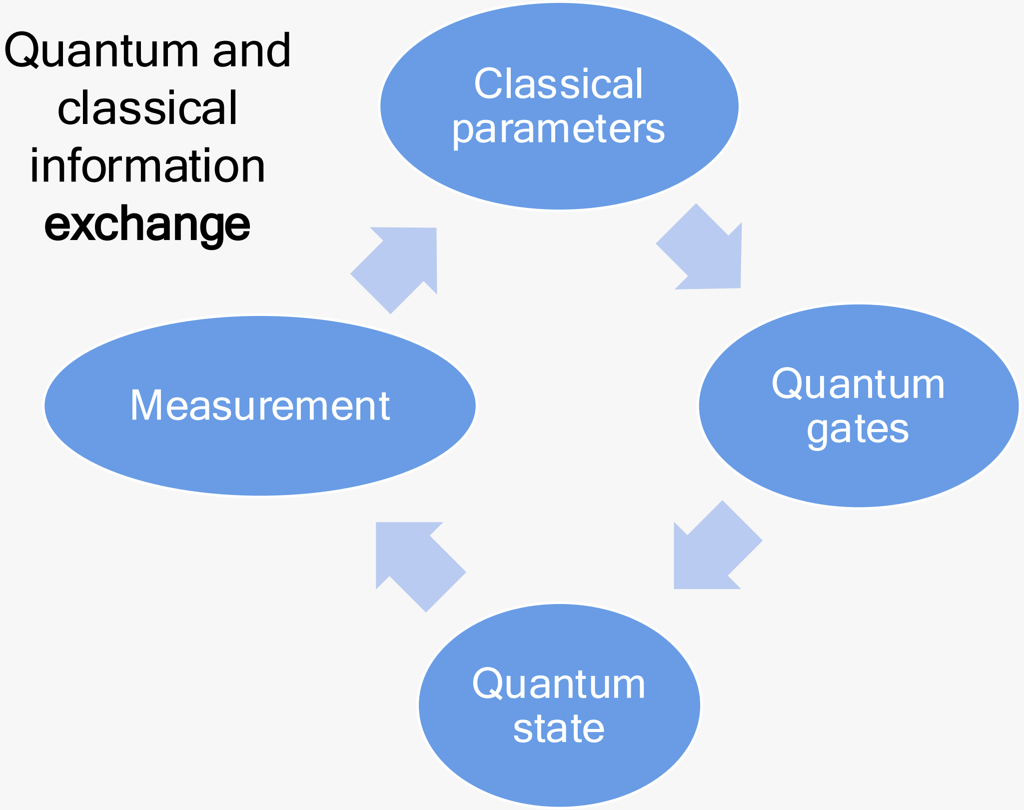
Variational Principle

- Many problems we might want to solve are expressed as a minimization (or maximization) problem:
  - Find a driving route that takes the least time
  - Find the lowest-energy configuration of electrons in a molecule
  - Minimize the risk in a stock portfolio
- Quantity we want to minimize is called a cost function
- Variational principle says:
  1. Make an educated guess for the solution
  2. Calculate the cost function
  3. The closer the cost function is close to its minimum value, the closer your guess is close to the true solution

IQM

Variational algorithms

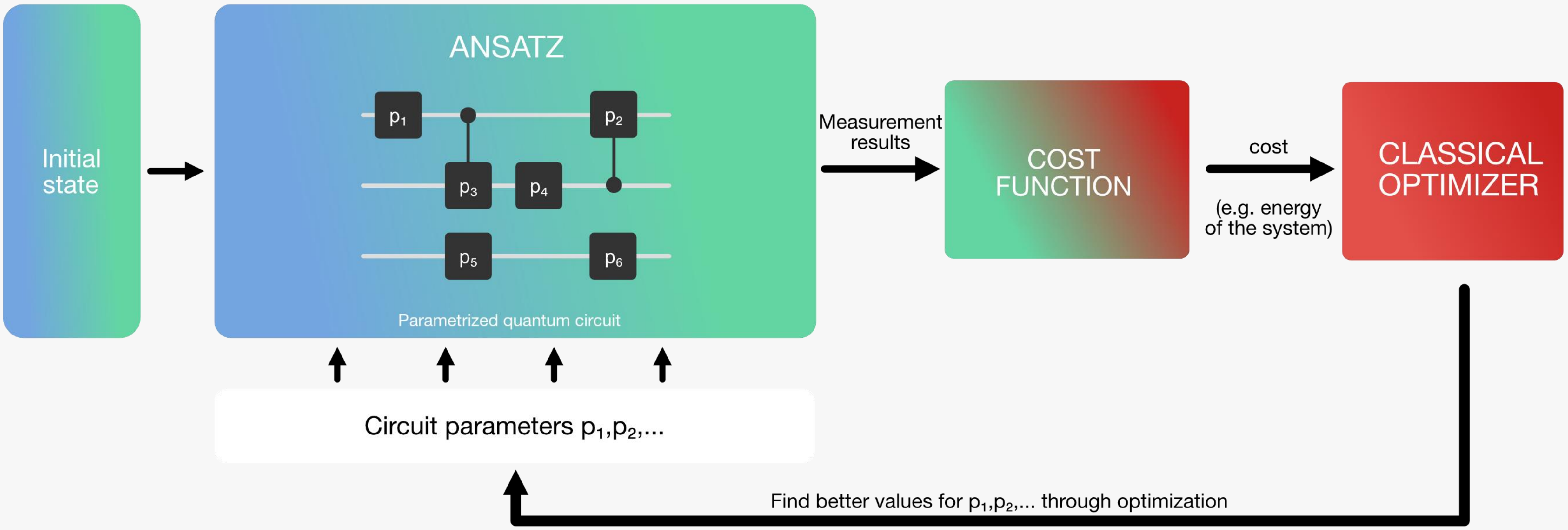
Use variational principle to find the best possible approximation of the true solution of our problem



Why is this interesting for **NISQ**?

- Hybrid computing resources
- Noise-resilient

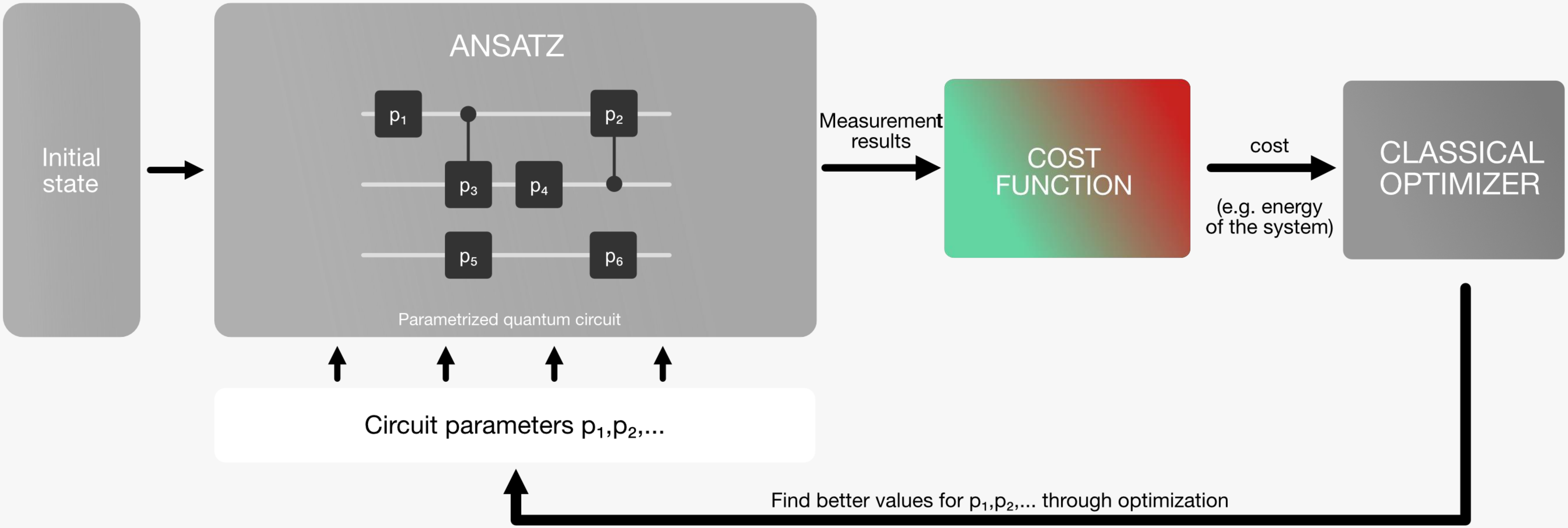
Variational algorithms are one way to do a hybrid algorithm



VERSATILE MODULAR STRUCTURE

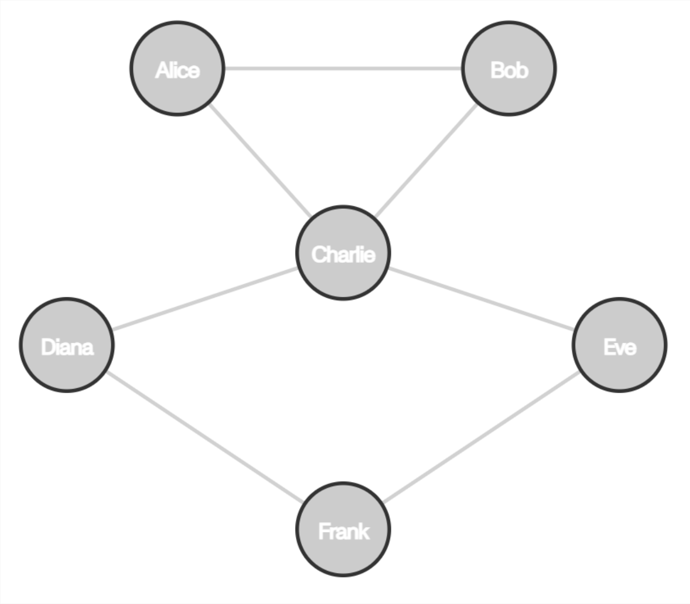
The cost function

The cost function



Max-Cut Problem

- You are proctoring an exam and need to divide the students into two rooms.
- Students who are friends with each other and in the same room are more likely to cheat.
  - Assume you know which students are friends.
- Goal: Assign each student a room to minimize the chance of cheating, that is, split up as many friendships as possible.



- Each dot (node) is a student.
- Each line (edge) is a friendship.

- NP-hard problem in general!

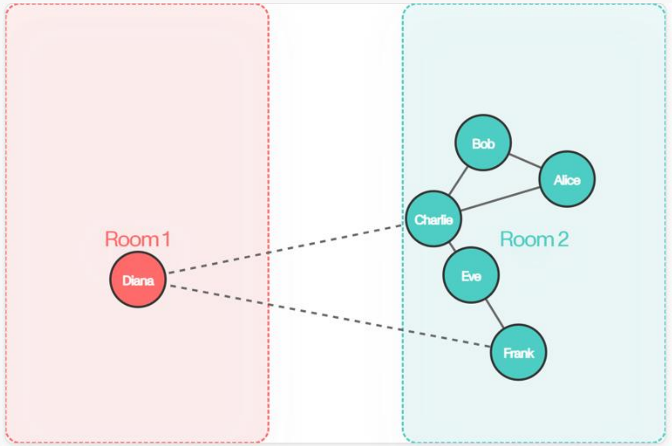
Cost functions

A cost function converts a guess at the answer into a single number

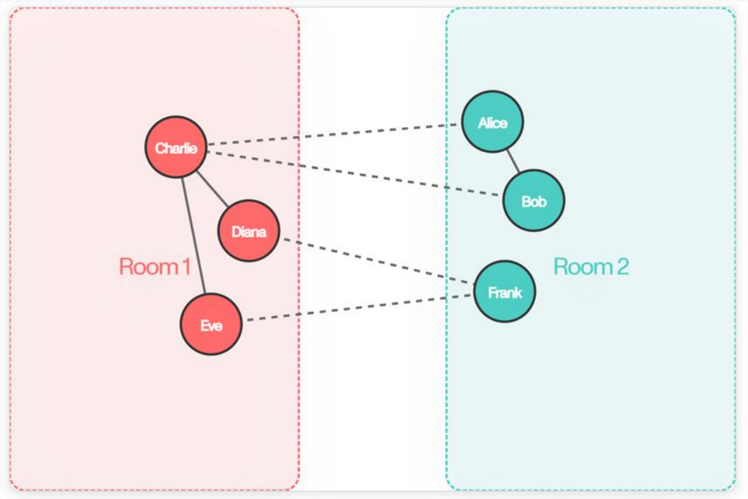
- The lower the output, the closer to the best solution you are

For MaxCut:

- Given: list of friendships
- Input: a guess of which students should be in which rooms
- Output: some number



Higher cost (e.g., 3)



Lower cost (e.g., -1)

Want to be able to calculate the cost function efficiently for any (quantum) input state on your QPU by making a measurement of some physical property of the qubits.

EXPERIMENT TIME!

Use the applet here https://tinyurl.com/iqm-students (or in the QR code) to play with the MaxCut problem. Can you figure out a way to encode the problem into a cost function?

Remember, the cost function takes as input:

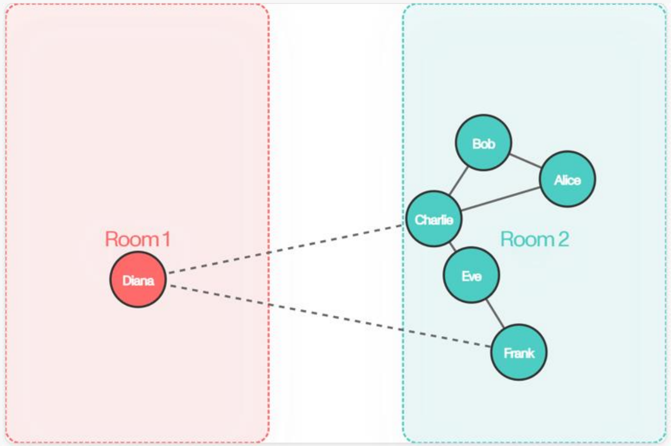
- The list of friendships
- A choice of room for each student

A cost function for Max-Cut

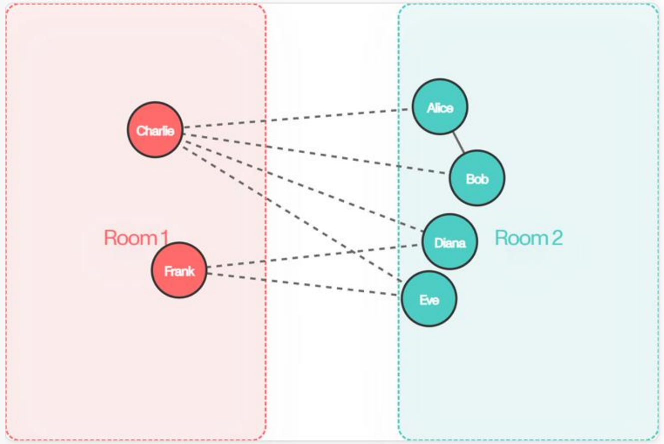
- Assign each student a qubit. $|0\rangle$ means that student is in room 0 and $|1\rangle$ means the student is in room 1.

- Define a cost function $H(Z_i) = \sum_{i,j} \begin{cases} 0 \text{ if } i,j \text{ are not friends} \\ Z_i Z_j \text{ if } i,j \text{ are friends} \end{cases}$
  - $Z_i = 1$ if qubit i is in state $|1\rangle$ $Z_i = -1$ and if qubit i is in state $|0\rangle$.
  - Friends in the same room contribute +1 to the cost function
  - Friends in different room contribute -1 to the cost function
  - $H(Z_i)$ is minimized when the number of split-up friendships is maximal.

- Turns out: this cost function is easy to calculate with a quantum computer



Cost = (5 unbroken) - (2 broken) = +3

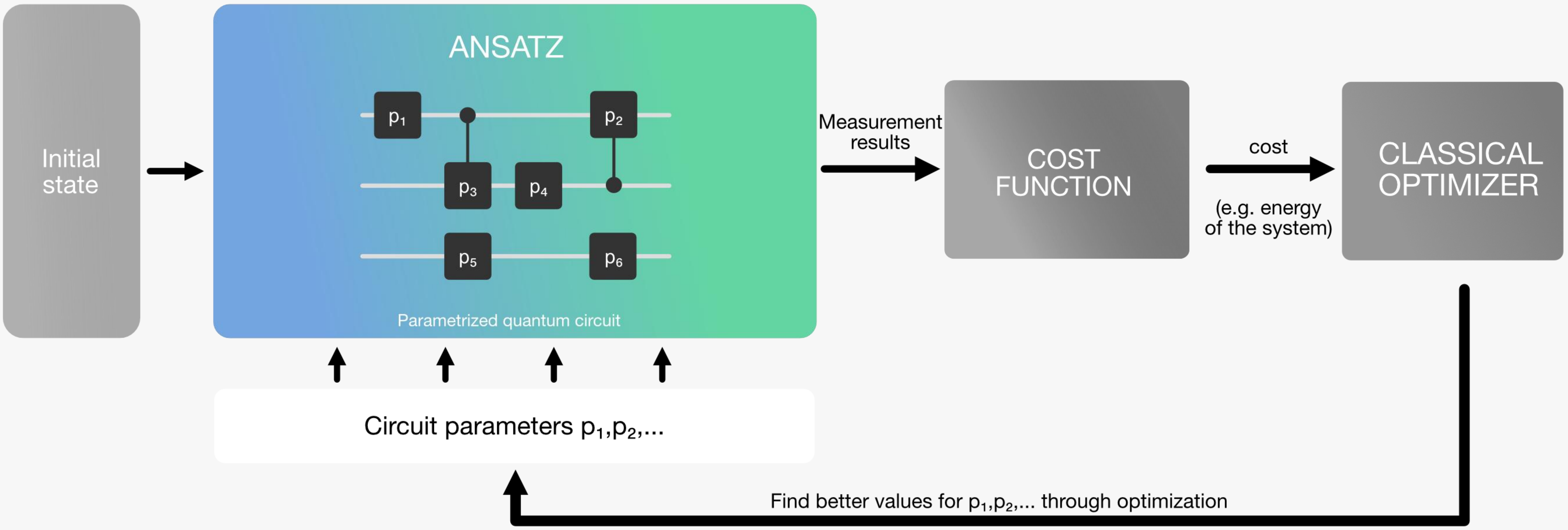


Cost = (1 unbroken) - (6 broken) = -5

IQM

The ansatz

The Ansatz


Initial state
ANSATZ
p1
p2
p3
p4
p5
p6
Parametrized quantum circuit
Measurement results
COST FUNCTION
cost
(e.g. energy of the system)
CLASSICAL OPTIMIZER
Circuit parameters p1,p2,...
Find better values for p1,p2,... through optimization

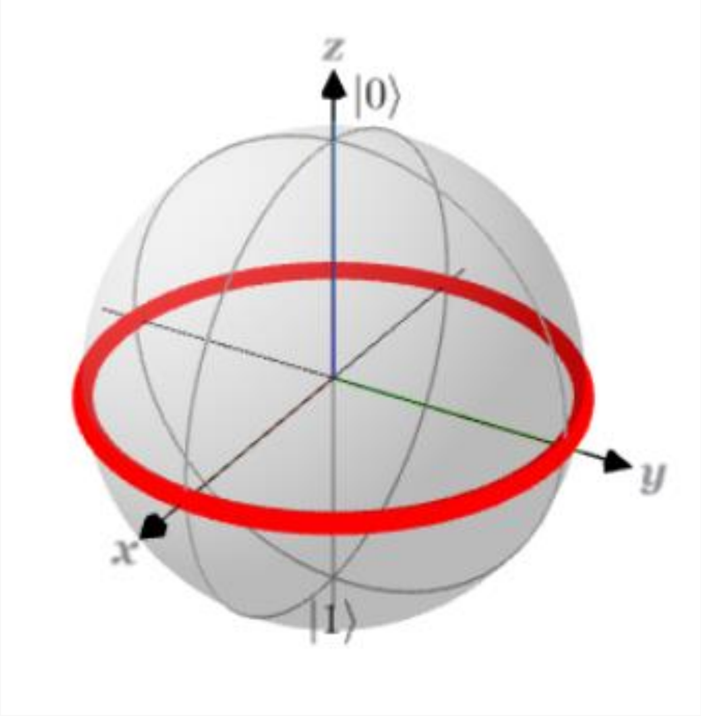
Goal of a variational algorithm

- Encode possible solutions to the minimization problem as quantum states
  - Sometimes this is natural – in quantum chemistry, the solution is often the quantum state of a bunch of electrons/atoms
- Find a quantum circuit that transforms some given initial state into the (approximate) solution of the minimization problem

- Infinitely many quantum circuits (and answer states) are possible! Can't try them all…

What is an ansatz?

Example:



- θ_2 is a classical parameter - can be any angle.
- An ansatz is a collection of guesses for the solution to a problem.
  - For us, an ansatz is a collection of quantum states (i.e. a collection of quantum circuits applied to some initial state)
  - Can be a random guess or an informed guess

QUIZ TIME!

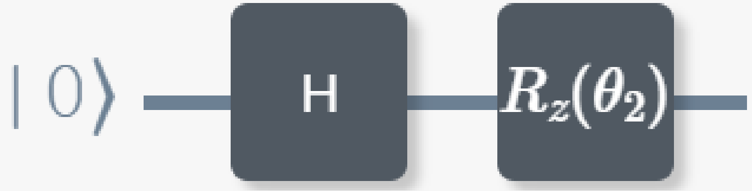
What properties might you want an ansatz to have?

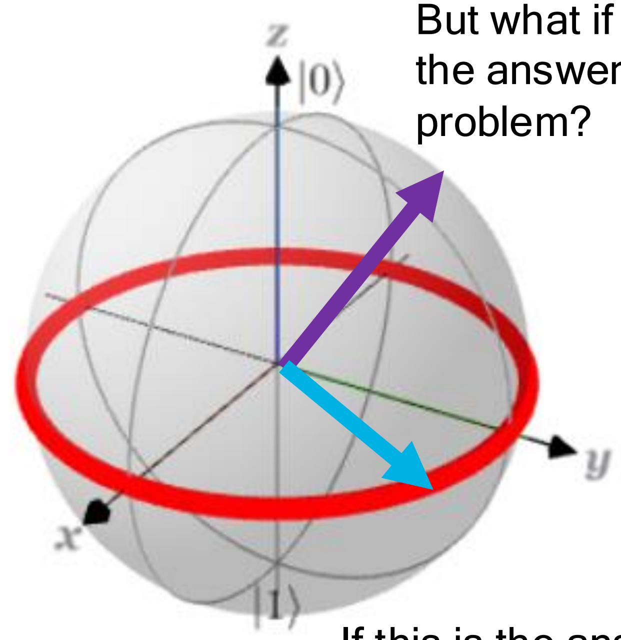
Some possible answers:

- Easy to compute with
- Should actually include the solution to the problem
- Easy for your quantum hardware to implement
- Not too many parameters

What is an ansatz?

Example:





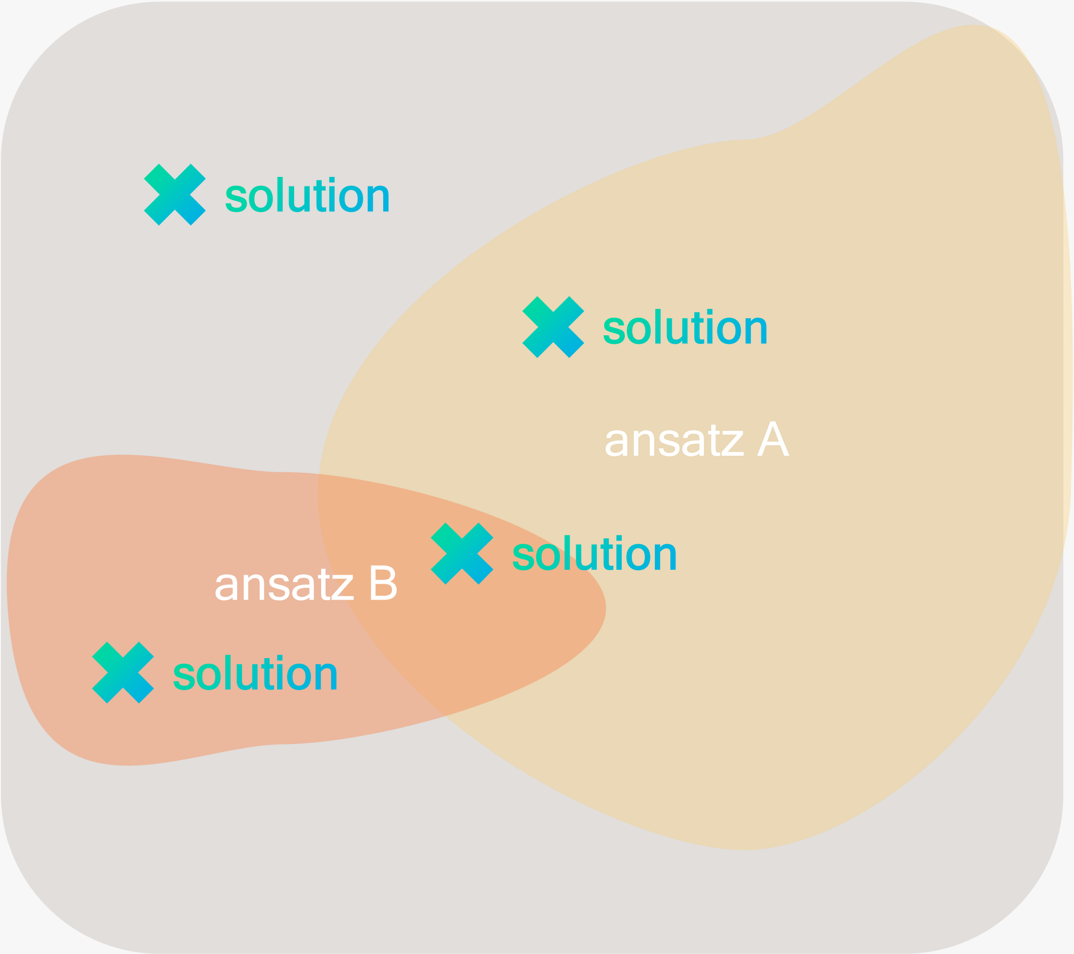
But what if this is the answer to our problem?

If this is the answer to our problem, this ansatz is useful!

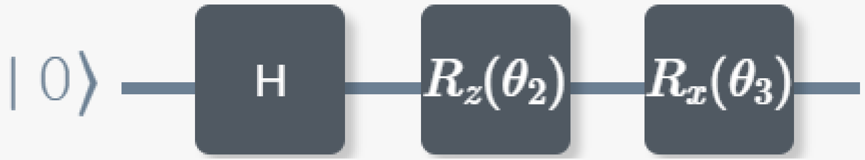
- θ_2 is a classical parameter - can be any angle.
- An ansatz is a collection of guesses for the solution to a problem.
  - For us, an ansatz is a collection of quantum states (i.e. a collection of quantum circuits applied to some initial state)
  - Can be a random guess or an informed guess

IQM

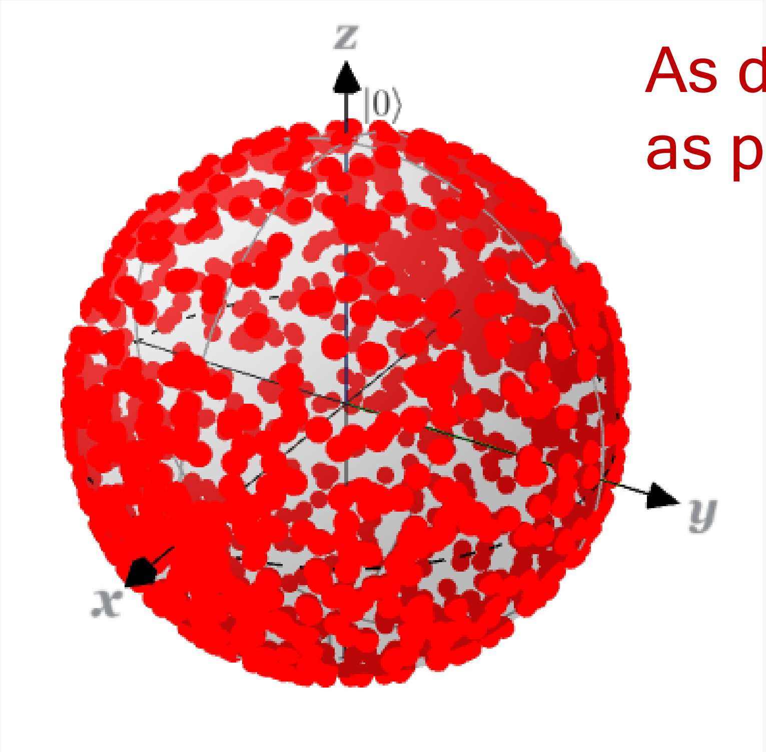
Complete set of quantum states



A more general ansatz



θ_2 and θ_3 are classical parameters.

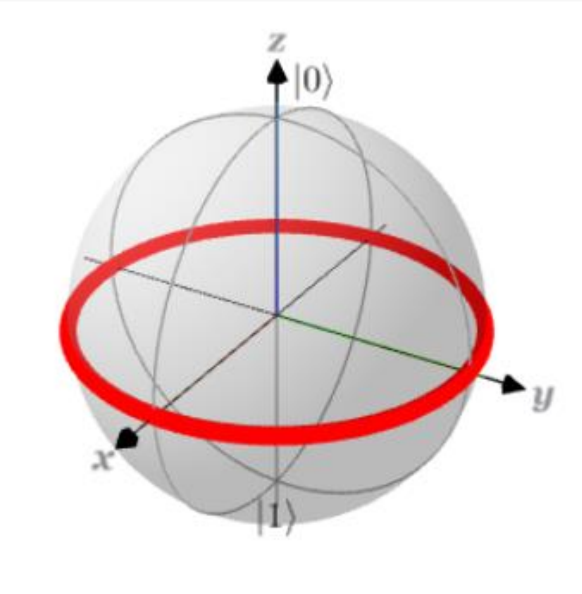


As dense as possible

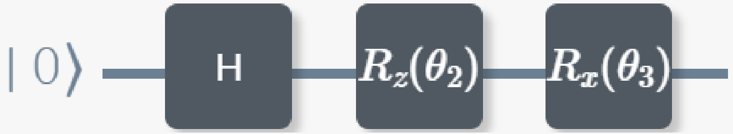
Even just choosing a few values of θ_2 and θ_3 lets us get close to any state!

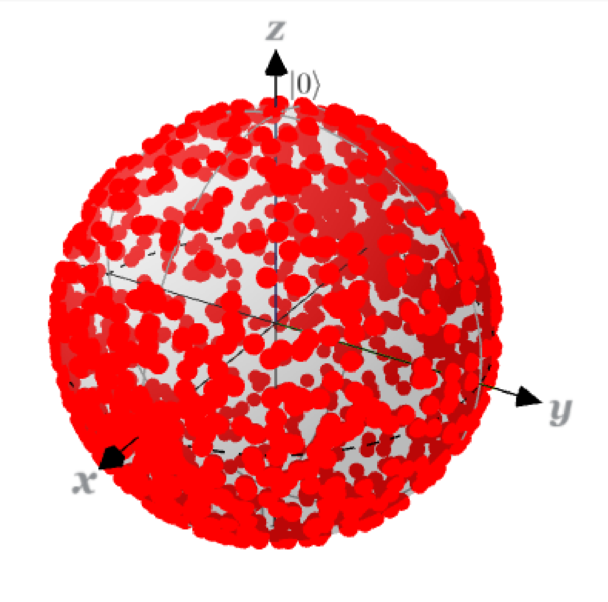
Expressibility

Expressibility is a measure of the power of an ansatz to generate a uniform set of states in the space of quantum states.



Low expressibility



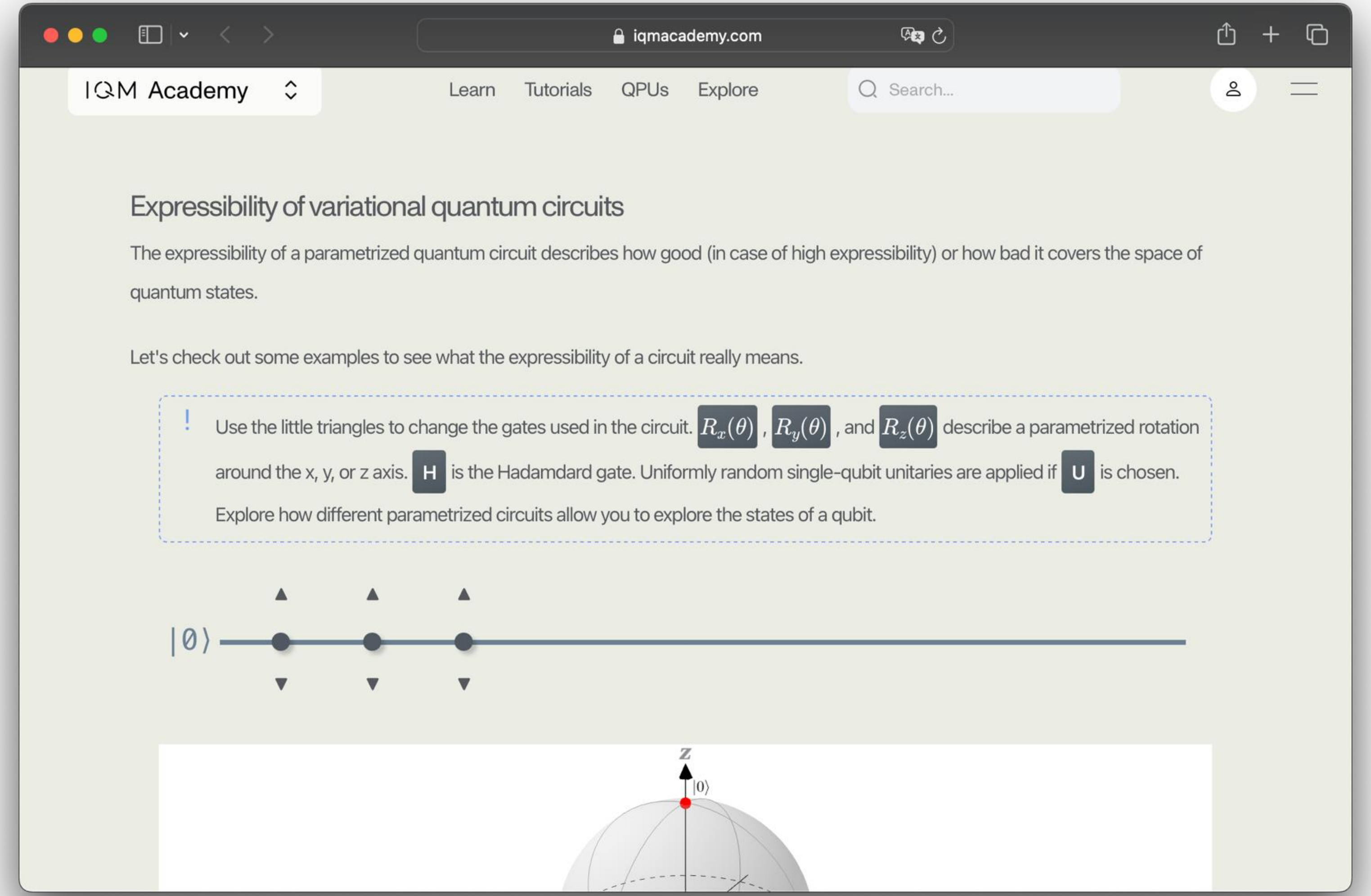


High expressibility

Open question:
How important is expressibility for VQA?

IQM

Try it out yourself



IQM

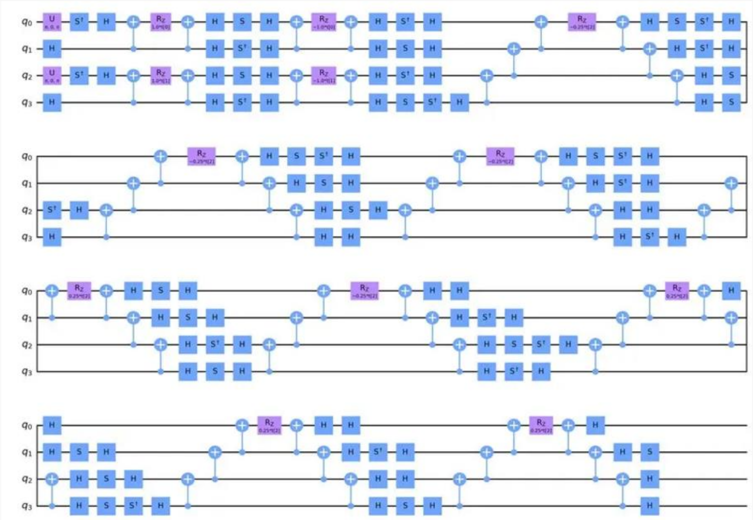
https://www.iqmacademy.com/play/expressibility

Types of Ansätze

Problem-inspired

Good for one problem, e.g. quantum chemistry

e.g. “Unitary Coupled Cluster” ansatz



Problem-agnostic

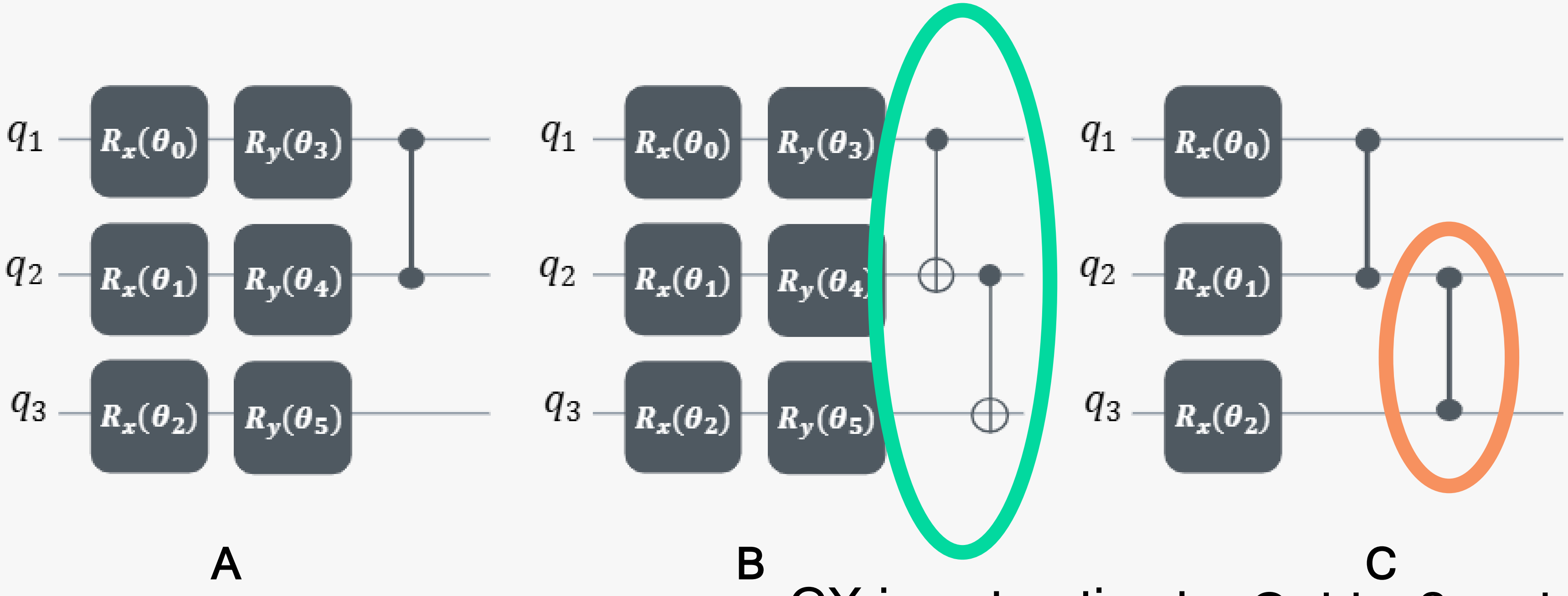
Hardware efficient

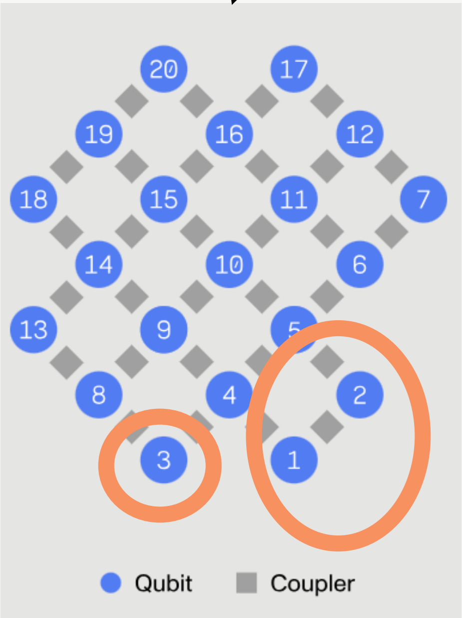
- Limit the depth
- Use native gates
- Take into account connectivity

Avoid overhead of transpilation

QUIZ TIME!

Which of the following circuits is hardware efficient for our Garnet QPU?

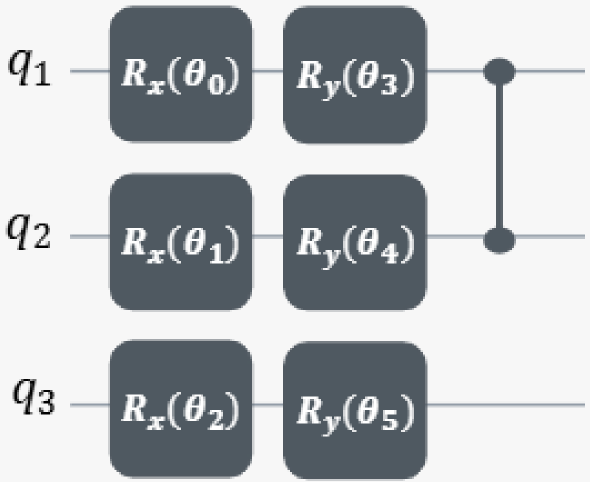


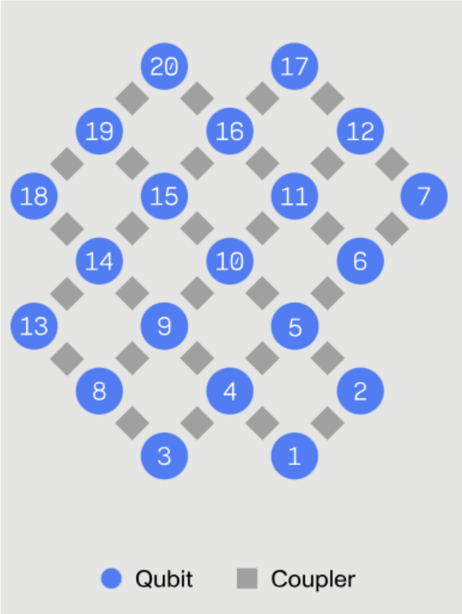


CX is not native to IQM hardware!

Qubits 2 and 3 aren't coupled on Garnet

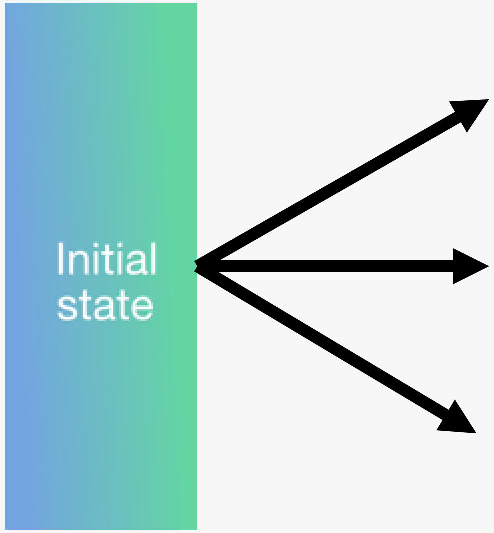
Correct answer





- This circuit includes only **native gates** for the QPU and uses CZ gates on qubits directly connected via a coupler.
- Note: The expressivity of this circuit is limited. It cannot express any state in which q_3 is entangled with q_1 and/or q_2.

Where to start?



No special requirements $|0\rangle^{\otimes N}$

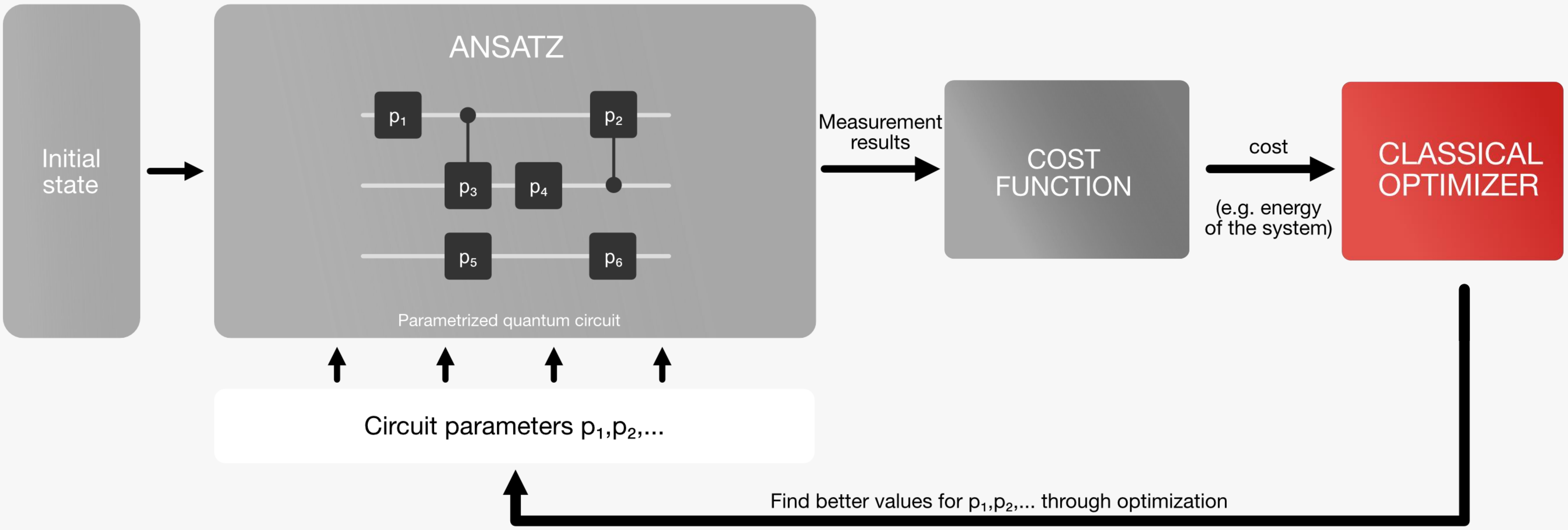
Reference state (e.g. Hartree-Fock in quantum chemistry)

Feature map (machine learning)

Initial state can also be random or educated guess.

The optimizer

The Optimizer



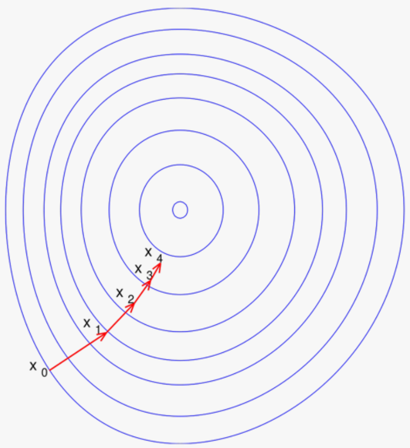
What is the role of the classical computer?

Determines how to adjust ansatz parameters to decrease the cost function

Gradient-based methods

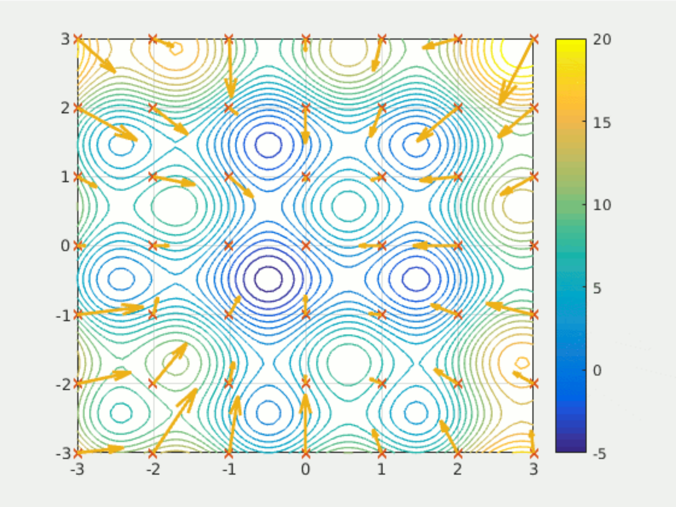
$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i - \eta \nabla C(\boldsymbol{\theta}_i)$$

Gradient tells us how to change the parameters to make C decrease as fast as possible. Think "go straight down the mountain."



Different methods are efficient to compute the gradient on classical vs. quantum computers. Most common: "parameter shift rules"

Gradient-free methods

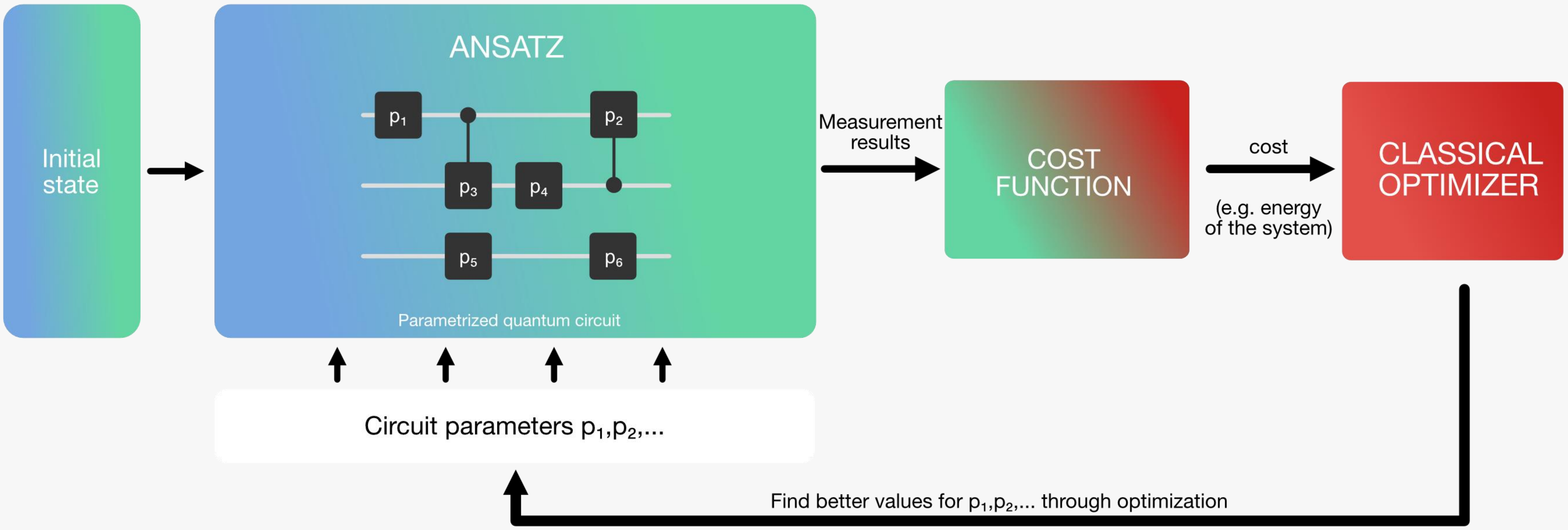


Example: particle swarm optimization

Image sources: Wikipedia

Well-known variational quantum algorithms

A hybrid algorithm



VERSATILE MODULAR STRUCTURE

IQM

Variational quantum eigensolver (VQE)

Goal: find the lowest energy state of a quantum system (e.g. molecules, materials).

How It Works:

- Express the problem's Hamiltonian (energy) H in qubit operators (atoms and electrons* aren't qubits!).
- Parameterized Ansatz: Prepare a quantum state $|\psi(\theta)\rangle$ using a variational circuit.
- Cost function: Evaluate the expectation value $\langle\psi(\theta)|H|\psi(\theta)\rangle$ (average energy) on a quantum computer.
- Classical Optimization: Update θ to minimize the energy.

Example applications

Molecular ground state energy estimation (e.g., H_2, LiH, BeH_2).

Material science and quantum chemistry.

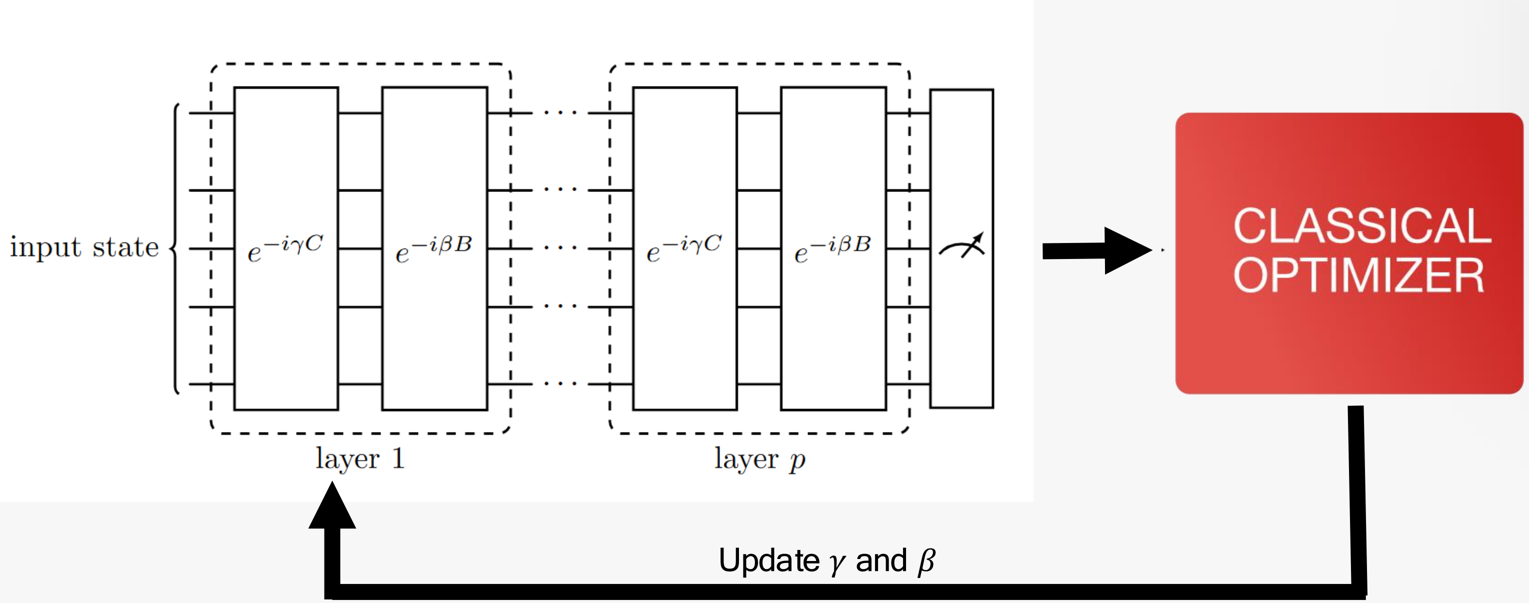
IQM

*Actually, electrons are "fermions" (obey the Pauli exclusion principle) and qubits are not. Encoding electrons as qubits requires some more sophisticated tools - read about the "Jordan-Wigner transformation" if you're interested.

Quantum Approximate Optimization Algorithm (QAOA)

Solve combinatorial optimization problems like MaxCut

How It Works



- Fix the number of layers p
- γ and β are the ansatz parameters
- C is a circuit implementing the cost function
- B is a “mixer” operator that adds “quantumness”

Example applications

- MaxCut
- Portfolio optimization
- Scheduling

Learn more in lab!

Conclusion

Conclusion: Variational quantum algorithms

Variational quantum algorithms are hybrid quantum-classical algorithms that use a parameterized quantum circuit (ansatz) and classical optimization to solve complex problems.

Key Components:

- Quantum Circuit (Ansatz): Encodes the problem into a quantum state.
- Cost Function: Represents the problem's objective, evaluated on a quantum computer.
- Classical Optimizer: Updates parameters to minimize (or maximize) the cost function.

Popular Algorithms:

- VQE (Variational Quantum Eigensolver): For finding ground states of Hamiltonians.
- QAOA (Quantum Approximate Optimization Algorithm): For solving combinatorial optimization problems.
- Variational Classifiers: For quantum machine learning tasks

Day 2 - Lab

Find the Day 2 lab here

https://tinyurl.com/d8359bvm

Don’t waste all your time trying to debug – spend more time trying to follow the demonstration and fill in the code yourself later!